Vũ Đình Cường *(Chủ biên)*
Phương Lan *(Hiệu đính)*

Từng bước khám phá an ninh mạng

TÌM LẠI PASSWORD

& phương pháp phục hồi an toàn dữ liệu

NHÀ XUẤT BẢN LAO ĐỘNG-XÃ HỘI

VŨ ĐÌNH CƯỜNG *(Chủ biên)*
PHƯƠNG LAN *(Hiệu đính)*

Từng bước khám phá an ninh mạng

TÌM LẠI PASSWORD

& phương pháp phục hồi an toàn dữ liệu

NHÀ XUẤT BẢN LAO ĐỘNG - XÃ HỘI

LỜI NÓI ĐẦU

Công nghệ Thông tin nói chung và Mạng máy tính nói riêng trong những năm gần đây phát triển mạnh mẽ, nhất là trong tình hình đất nước hội nhập và mở cửa. Tuy nhiên, trên đà phát triển đó cũng nảy sinh nhiều vấn đề bất cập và thách thức như cơ sở hạ tầng của chúng ta còn yếu kém, nguồn nhân lực kỹ thuật cao còn thiếu.

Để góp phần vào sự phát triển chung của nền khoa học máy tính nước nhà, chúng tôi giới thiệu đến Quý độc giả bộ sách **"Từng bước khám phá an ninh mạng"**. Sách cung cấp những kiến thức cơ bản nhất và cần thiết nhất để trở thành một Nhân viên quản trị mạng, Quản trị bảo mật. Đặc biệt, bộ sách này sẽ hướng các bạn trở thành một White Hat Hacker, với phương châm "Học hack để chống lại Hack", cũng như trong binh pháp có câu "Biết người, biết ta. Trăm trận, trăm thắng".

Bộ sách **"Từng bước khám phá an ninh mạng"** được chia thành nhiều tập, mỗi tập được chia thành nhiều chương, mỗi chương giải quyết trọn vẹn một vấn đề nào đó. Trong mỗi tập đều được bố cục chặt chẽ, phần đầu là tên chương, tiếp theo là những tiêu mục chính cần giải quyết trong chương, sau đó là những tóm tắt tổng hợp của chương. Sau cùng là phần giải quyết vấn đề.

Sự bố cục chặt chẽ và khoa học này sẽ giúp bạn đọc nhanh chóng nắm bắt được những vấn đề và tìm nhanh được những mục mà độc giả thực sự quan tâm. Bạn đọc không cần mất nhiều thời gian lật sách tới phần mục lục mà vẫn có thể biết được sơ đồ và bố trí của chương.

Tập ba mang tên **"Tìm lại Password và Phương pháp Phục hồi – An toàn Dữ liệu"**. Tập này được chia làm 6 chương, tương ứng với từng chương là những vấn đề nóng bỏng của Tin học hiện nay. Mỗi vấn đề nêu ra trong từng chương đều gắn bó sâu sắc với tình hình thực tế và được giải quyết một cách triệt để, rõ ràng. Mỗi thao tác đều có hình ảnh minh họa cụ thể. Phương pháp trình bày theo kiểu từng bước phù hợp với mọi đối tượng độc giả từ căn bản đến nâng cao.

Chương 1: Tập trung giải quyết các vấn đề liên quan đến Email như: Một số thủ thuật Yahoo Messenger, cách xác định vị trí địa lý của email, Mail server, cách sử dụng một số phần mềm Spam, gửi thư nặc danh bằng Ghost mail, phương pháp chống Bomb mail.

Chương 2: Giải quyết triệt để các vấn đề liên quan đến password Windows, từ cách reset password khi lỡ quên hoặc bị Hack cho đến những phương pháp tìm lại mật khẩu bằng những phần mềm lớn và phức tạp. Ở chương này chúng tôi tuyển chọn và giới thiệu một số phần mềm tìm password mạnh nhất và thông dụng nhất hiện nay.

Chương 3: Tập trung giải quyết các vấn đề về password tập tin như: Tìm lại password các tập tin của MS Office (.doc, .xls, .xlsx, .ppt, .mdb), các tập tin nén của Winzip, Winrar, tập tin .pdf (Adobe). Ngoài ra, chương này còn hướng dẫn bạn cách đặt những mật khẩu an toàn cho tập tin.

Chương 4: Hướng dẫn bạn đọc các phương pháp phục hồi dữ liệu, tập tin đã mất. Những tập tin bạn đã vô tình xóa hoặc tập tin bị mất do các tác nhân phá hoại như virus, trojan hay các hình thức phá hoại của đối thủ cạnh tranh. Ngoài ra, chương này còn giới thiệu đến bạn các phương pháp phục hồi dữ liệu ngay trên những phân vùng đã bị xóa, những ổ đĩa đã fdisk hay format.

Chương 5: Tập trung giải quyết các vấn đề về an toàn dữ liệu. Hướng dẫn bạn cách xóa sạch các tài liệu mật, dữ liệu riêng tư theo chuẩn Quốc tế.

Chương 6: Giới thiệu phương pháp cơ bản giúp nhanh chóng xóa sạch các dấu vết trong máy tính.

Phần mềm giới thiệu trong tập ba này đều được cung cấp trên website www.minhkhai.com.vn, tất cả đều có Licences, Serial, Keygen, CD Key, Crack hoặc Patch.

Mặc dù sách đã được biên tập kỹ, nhưng những thiếu sót là không thể tránh khỏi. Mọi góp ý và thắc mắc xin vui lòng liên hệ theo địa chỉ e-mail: mk.pub@minhkhai.com.vn.

MK.PUB

THƯ NGỎ

Kính thưa quý Bạn đọc gần xa!

Trước hết, Ban xuất bản xin bày tỏ lòng biết ơn và niềm vinh hạnh được đông đảo Bạn đọc nhiệt tình ủng hộ tủ sách MK.PUB.

Trong thời gian qua chúng tôi rất vui và cảm ơn các Bạn đã gửi e-mail đóng góp nhiều ý kiến quý báu cho tủ sách.

Mục tiêu và phương châm phục vụ của chúng tôi là:

- Lao động khoa học nghiêm túc.
- Chất lượng và ngày càng chất lương hơn.
- Tất cả vì Bạn đọc.

Một lần nữa, Ban xuất bản MK.PUB xin kính mời quý Bạn đọc tiếp tục tham gia cùng chúng tôi để nâng cao chất lượng sách. Cụ thể:

Trong quá trình sử dụng sách, nếu quý Bạn phát hiện thấy bất kỳ sai sót nào (*dù nhỏ*) xin đánh dấu, ghi chú nhận xét ý kiến của Bạn ra bên cạnh rồi gửi cuốn sách này cho chúng tôi theo địa chỉ:

Nhà sách Minh Khai

249 Nguyễn Thị Minh Khai, Q.I, Tp. Hồ Chí Minh.

E-mail: *mk.book@minhkhai.com.vn* hoặc *mk.pub@minhkhai.com.vn*

Chúng tôi xin hoàn lại cước phí bưu điện và gửi trả lại Bạn cuốn sách cùng tên. Ngoài ra chúng tôi còn gửi tặng Bạn một cuốn sách khác trong tủ sách MK.PUB. Bạn có thể chọn cuốn sách này theo danh mục thích hợp sẽ gửi tới Bạn.

Với mục đích ngày càng nâng cao chất lượng tủ sách MK.PUB, chúng tôi rất mong nhận được sự hợp tác nhiệt tình của quý Bạn đọc gần xa.

"MK.PUB cùng Bạn đọc đồng hành" để nâng cao chất lượng sách.

Một lần nữa chúng tôi xin chân thành cảm ơn.

MK.PUB

MỤC LỤC

LỜI NÓI ĐẦU 3
THƯ NGỎ 5
MỤC LỤC 6
Chương 1: E-MAIL HACK 11
I. Các thủ thuật trên Yahoo Messenger 11
1. Kích hoạt firewall *13*
2. Không cho phép tự động xem webcam *13*
3. Không Chat với người ngoài Friend List *14*
4. Ngăn chặn Kick Boot *15*
5. Loại bỏ quảng cáo dạng flash trong phần Plug-ins *15*
6. Chat nhiều nick với Yahoo 8.0 ..... *17*
7. Loại bỏ quá trình cập nhật (Update) *18*
II. Bomb mail và gửi thư nặc danh 18
1. Mail Nuker version 1.0 ..... *19*
2. Gửi thư nặc danh bằng Ghost mail *20*
3. Phương pháp chống thư rác và Bomb mail *22*
III. Các chương trình hỗ trợ E-mail 30
1. E-mail Spider *30*
2. E-Mail Tracker Pro Version 7.0 ..... *31*
3. Visual Route Version 7.1 ..... *33*
Chương 2: TÌM LẠI PASSWORD WINDOWS 37
I. Tìm hiểu về password 38
1. Các loại password *38*
2. Tìm hiểu về Shadow Password *38*
3. Password Windows *40*
II. Sao chép tập tin hệ thống bằng chương trình Volkov Commander 4.99 41
III. Active Password Changer 3.0.0.420 (NT/2000/XP/2003/Vista) 44
IV. L0pCrack 5.02 48
1. Tìm lại password Windows trên máy tính cục bộ *48*
2. Tìm lại password bằng từ điển *51*
3. Tìm password Windows từ tập tin SAM *54*

4. Tìm lại password Windows Server 2003 qua LAN 55
V. Windows Password Cracker V. 2.1.9.0 57
1. Tìm lại password bằng phương pháp Brute-force 57
2. Tìm Password bằng từ điển 60
3. Mã hóa dữ liệu 62
VI. Advanced Windows Password Recovery 2.9.2.224 62
1. Xác định password đăng nhập 63
2. Xác định thông tin chia sẻ 64
3. Tạo từ điển và Brute-force 66
4. Những chức năng nâng cao 68
VII. Proactive Windows Security Explorer™ 69
1. Tài khoản và password trên máy tính cục bộ 70
2. Xác định password từ tập tin SAM và SYSTEM 71
3. Xác định password qua LAN 73
VIII. Xem password đằng sau dấu sao (*) 75
1. See Password 75
2. Xem password bằng chương trình Asterisk Key 75
Chương 3: TÌM LẠI PASSWORD TẬP TIN 77
I. Tìm lại password trên tập tin của Winrar 77
1. Chương trình Rar Password Recovery 77
2. Advanced Rar Password Recovery 81
II. Tìm lại password trên tập tin của Winzip 81
1. Advanced Zip Password Recovery 81
III. Tìm lại password tập tin nén 85
1. Advanced Archive Password Recovery 3.01 85
2. Ultimate ZIP Cracker 85
IV. Tìm password các tập tin của MS Office 86
1. Accent Access Password Recovery 86
2. Accent Office Password Recovery 87
3. Accent Excel Password Recovery 94
4. Excel Password Recovery 94
5. MS Outlook Password Recovery 100
V. Tìm password các tập tin của Adobe Acrobat Reader (pdf) 101
1. PDF Password Cracker Pro V.3.0 101

2. Advanced PDF Password Recovery Pro V.2.0.4 ..... *104*
VI. Đặt password cho tập tin 105
1. Đặt password cho những tập tin của MS Word 2007 ..... *105*
2. Đặt password cho các tập tin của MS Excel 2007 ..... *106*
3. Đặt password cho các tập tin của MS PowerPoint 2007 ..... *107*
4. Đặt password cho các tập tin của MS Access 2007 ..... *109*
5. Đặt password cho tập tin .pst của MS Outlook Express 2007 ..... *110*
6. Đặt password cho tập tin của Winzip và Winrar *111*
7. Đặt password cho các tập tin của Adobe Acrobat Reader (pdf) ... *116*
Chương 4: PHỤC HỒI DỮ LIỆU ĐÃ MẤT **119**
I. Tìm hiểu về quá trình lưu trữ 119
II. Ontrack Easy Data Recovery Professional 120
1. Chẩn đoán dữ liệu trên đĩa *120*
2. Phục hồi dữ liệu đã mất *124*
3. File Repair *136*
4. Email Repair *138*
III. Chương trình Get Data Back for NTFS 138
1. Sử dụng những thiết lập mặc định *139*
2. Phục hồi thông tin bị mất do Fdisk hay Format *143*
IV. Get Data Back for FAT 146
1. Tìm lại tập tin đã xóa *146*
V. Data Doctor Recovery - NTFS-FAT 149
1. Standard Search *150*
2. Advanced Search *152*
VI. PhotoRescue Professional 154
VII. Một số chương trình phục hồi dữ liệu khác 157
1. Active@ Undelete *157*
2. Final Recovery *157*
3. Power Data Recovery *157*
4. Data Recovery Wizard Professional 3.3.4 ..... *157*
5. Recover My Files *157*
6. Partition Recovery 2.0 ..... *158*
7. BadCopy Pro *158*

Chương 5: AN TOÀN DỮ LIỆU 159
I. Tìm hiểu về an toàn dữ liệu 160
1. Cảnh báo về việc xóa dữ liệu 160
2. Đôi điều về lệnh Delete và Format 160
3. Làm sao để bảo mật thông tin 161
4. Các phương pháp tẩy sạch dữ liệu an toàn 161
II. BPS Data Shredder 162
1. Shred Drives 162
2. Shred Files 163
3. Shred Folder 164
4. Shred Recycle bin 165
5. Schedule 166
III. Track Eraser Pro 168
1. Các tùy chọn của chương trình 169
2. Những thiết lập liên quan đến quá trình xóa dữ liệu 172
3. Xóa thư mục và tập tin chỉ định 177
4. Xóa nhanh những mục chọn 179
IV. Một số chương trình bảo mật khác 179
1. R-Wipe and Clean 179
2. Directory Snoop 180
3. East-Tec Eraser 2007 180
4. Clean Space Ultimate 180
5. Privacy Eraser Pro 181
6. BCWipe 3.0 181
7. Clean Disk Security 181
8. Secure Clean PC 182
Chương 6: XÓA DẤU VẾT BẰNG PHƯƠNG PHÁP THỦ CÔNG ... 183
I. Một số dấu vết trong máy tính 184
1. Tìm hiểu về Cookies 184
2. Vị trí lưu trữ của Cookies 184
3. Tìm hiểu về Temporary Internet Files 186
4. Vị trí lưu trữ của Temporary Internet Files trong máy tính 186
5. Tìm hiểu về History 186

6. Vị trí lưu trữ của History *187*
7. Tìm hiểu về những tập tin Temporary *187*
8. Vị trí lưu trữ của Temporary *187*
9. Những tập tin mới mở *188*
10. Loại bỏ dấu vết trong Registry của Windows *189*
11. Loại bỏ một số thông tin trong Registry *189*
II. Xóa dấu vết mở tập tin 192
1. Xóa những thông tin trong thư mục Recent *192*
2. Xóa những thông tin trong Event Viewer *194*
III. Xóa dấu vết trong trình duyệt Internet Explorer 195
1. Xóa Cookies *195*
2. Xóa History *196*
IV. Xóa dấu vết trong trình duyệt Mozilla Firefox 197
1. Xóa Cookies *198*
2. Loại bỏ History *199*
V. Xóa dấu vết trong trình duyệt Netscape Navigator 200
1. Xóa Cookies *201*
2. Xóa History *202*
VI. Xóa dấu vết trong trình duyệt Safari 203
1. Loại bỏ Cookies *203*
2. Xóa History *204*
VII. Xóa dấu vết trong trình duyệt Flock 205
VIII. Xóa dấu vết trong trình duyệt Green Browser 205
1. Loại bỏ Cookies *206*
2. Xóa History *207*
IX. Xóa dấu vết trong trình duyệt Opera 207
1. Xóa Cookies *207*
2. Xóa History *209*

Chương 1:

E-MAIL HACK

- **Các thủ thuật trên Yahoo Messenger.**
- **Bomb mail và gửi thư nặc danh.**
- **Các chương trình hỗ trợ E-mail.**

Ngày nay, với sự phát triển mạnh mẽ của Internet nên việc trao đổi thông tin - liên lạc được thực hiện một cách nhanh chóng và không phụ thuộc vào vị trí địa lý nữa. Gửi và nhận email chỉ mất một vài giây. Ngoài ra, qua dịch vụ Internet ta có thể gặp gỡ, hẹn hò trực tuyến với nhau qua dịch vụ Chat miễn phí.

Tuy nhiên, mỗi dịch vụ phát triển đều có các hạn chế, có những lỗ hổng bảo mật mà từ đó hacker có thể dễ dàng khai thác để tấn công. Đối với email, ta thường thấy nhất là hình thức gửi thư rác (thường gọi là Spam) do các Spammer gây ra, hình thức Bomb mail do các Bomber gửi. Đối với dịch vụ Chat thường xuất hiện hình thức kick boot, ...

Ngoài ra, xác định nguồn gốc và vị trí địa lý của một email cũng là vấn đề nóng bỏng và đang rất được quan tâm hiện nay. Khi đang Chat với một ai đó mới quen trong Room Chat, nhưng khi hỏi họ ở đâu, thì họ nói rằng họ ở Bắc cực hay một nước Châu phi xa xôi nào đó. Trong khi đó, có thể họ chỉ ngồi bên cạnh bạn hoặc là một đồng nghiệp làm chung trong Công ty. Vậy làm thế nào để xác định được vị trí của người bạn mới này. Hay làm thế nào để biết được vị trí của một Mail Server?

Chương này sẽ giải quyết trọn vẹn các vấn đề trên, giới thiệu một số phần mềm hỗ trợ Email và Chat.

I. Các thủ thuật trên Yahoo Messenger

Yahoo Messenger được xem là chương trình giao lưu trực tuyến được ứng dụng rộng rãi nhất trên Internet hiện nay. Ngoài tính năng Chat thông thường, Yahoo còn hỗ trợ Voice Chat và Webcam rất tiện lợi. Tuy nhiên, khi sử dụng chương trình này cũng thường gặp rất nhiều vấn đề

không tốt như: Sex – Webcam, Kick boot, gửi thông điệp quảng cáo bừa bãi, những ngôn từ thô tục, phản động,...

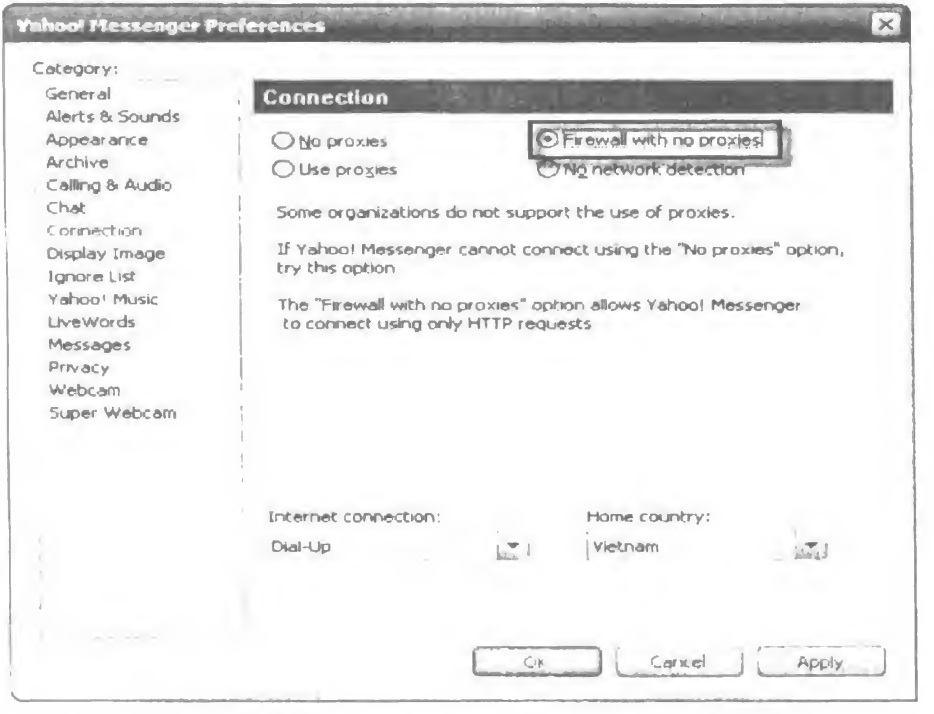
Để ngăn chặn các hình thức tấn công này, ta chỉ cần kích hoạt Firewall của Yahoo. Tuy nhiên, nếu kích hoạt Firewall thì sẽ không sử dụng tính năng Voice – Chat được nữa.

Để hiểu rõ hơn về các mục được đề cập trong các phần sau, chúng ta hãy tìm hiểu một số khái niệm.

- **Kick boot:** Là quá trình gửi liên tiếp các thông điệp đến Nick của nạn nhân qua Yahoo Messenger. Các thông điệp này không ngừng tăng lên cho đến khi máy tính của nạn nhân bị treo. Khi muốn sử dụng lại máy tính, nạn nhân phải khởi động lại.
- **Sex – Webcam:** Là quá trình phát tán những Webcam có nội dung không lành mạnh qua Yahoo Messenger. Các chương trình quảng cáo không lành mạnh thường lợi dụng những webcam này để đính kèm các thông điệp quảng cáo.
- **Spammer:** Là những người phát tán các thông điệp quảng cáo qua Internet, bằng cách gửi email đến nạn nhân. Một số email thường chứa Virus, Trojan, những thông tin không lành mạnh nhằm theo dõi và lấy thông tin từ nạn nhân.
- **Bomber:** Là một người nào đó sử dụng các chương trình đặc biệt, để gửi nhiều thông điệp hoặc email đến một Nick name hay hộp thư nào đó nhằm gây treo máy hoặc tràn hộp thư của nạn nhân. Một số Bomber còn lợi dụng hình thức đánh bomb để cài đặt virus hoặc trojan vào máy tính nạn nhân.
- **Scammer:** Là những kẻ lừa đảo, chúng dựng lên những mô hình kinh tế như: Ngân hàng, Công ty, hay một tổ chức nào đó nhằm lấy tiền của đối tác hoặc các thành viên tham gia.
- **Fishing:** Có nghĩa là lừa đảo, giả mạo, nhằm mục đích là khai thác thông tin người dùng. Các trang fishing thường gặp nhất là các trang web có mục đăng nhập được ngụy trang giống các trang web lớn như: Ebay, Paypal, E-gold. Tuy nhiên, tên miền của chúng được đặt tên gần giống với địa chỉ website chính thức nhằm đánh lừa, qua mắt nạn nhân. Ví dụ, trang web của E-gold có địa chỉ là e-gold.com thì Hacker sẽ tìm các tên miền (domain) gần giống như: e-gold-login.com, egold.com.

1. Kích hoạt firewall

1. Đăng nhập Nick của bạn vào Yahoo Messenger.
2. Sau khi đăng nhập thành công, vào menu **Messenger > Preferences > Connection.**
3. Nhấp chọn vào mục **Firewall with no proxies**, tiếp theo nhấp **OK** để áp dụng (xem hình 1 1).

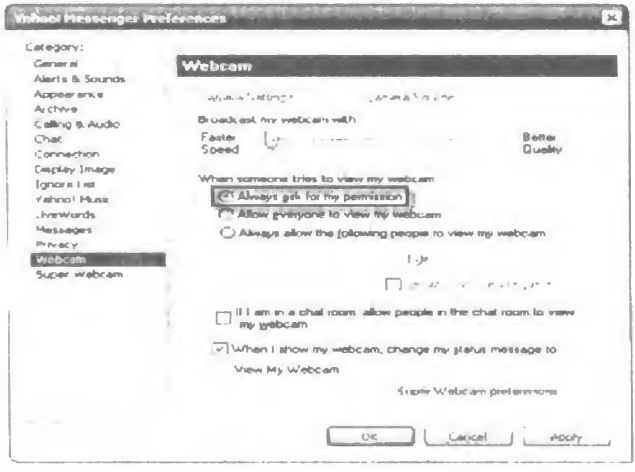


Hình 1.1: *Chọn Firewall with no proxies.*

2. Không cho phép tự động xem webcam

Để ngăn chặn những Nickname không rõ tự động xem Webcam khi chưa được phép, thực hiện như sau:

1. Đăng nhập Nick của bạn vào Yahoo Messenger.
2. Sau khi đăng nhập thành công, vào menu **Messenger > Preferences > Webcam**.
3. Nhấp chọn vào mục **Always ask for my permission**, tiếp theo nhấp **OK** để áp dụng (xem hình 1.2).



Hình 1.2: *Chọn Always ask for my permission.*

3. Không Chat với người ngoài Friend List

Để tránh người không rõ danh tính, không có trong friend list của bạn, hay những website quảng cáo làm phiền, bạn thực hiện như sau:

1. Đăng nhập vào Yahoo Messenger.
2. Sau khi đăng nhập thành công, vào menu **Messenger > Preferences > Ignore List**.
3. Nhấp chọn vào mục **Ignore anyone who is not on my Messenger List**.

Mục này có chức năng làm ngơ trước những người không có trong friend list của bạn (xem hình 1.3).

Hình 1.3: *Không chat với những người ngoài friend list.*

4. Ngăn chặn Kick Boot

Kick Boot là phương pháp mà Attacker thường dùng để tấn công vào máy tính của người dùng Yahoo Messenger. Nó hoạt động bằng cách gửi liên tiếp các thông điệp hoặc đá văng Nick của người dùng ra khỏi Yahoo Messenger. Để ngăn chặn, bạn thực hiện như sau:

1. Đăng nhập vào Yahoo Messenger.
2. Sau khi đăng nhập thành công, vào menu **Messenger > Preferences > Chat**.
3. Nhấp chọn vào mục **Ignore chat invitations** (xem hình 1.4).

Mục này được chọn sẽ bỏ qua những lời mời vào Room Chat, điều này giảm thiểu những cửa sổ được hiển thị khi Chat. Nếu máy tính của bạn có cấu hình yếu thì sẽ dẫn đến tình trạng treo máy, hoặc có những chương trình như Virus hoặc Trojan tự động được cài vào máy tính.

Hình 1.4: *Chọn Ignore chat invitations.*

5. Loại bỏ quảng cáo dạng flash trong phần Plug-ins

5.1. Đối với Yahoo Messeneger 8.0.0.683

Để loại bỏ quảng cáo dạng này, bạn thực hiện như sau:

1. Vào thư mục **C:\ > Program Files > Yahoo! > Messenger > Cache**.

2. Mở tập tin **urls.xml** bằng **Nodepad**, tiếp theo xóa tất cả nội dung có trong tập tin này, sau đó nhấn **Ctrl + S** để lưu những thay đổi (xem hình 1.5).

Hình 1.5: *Xóa nội dung tập tin urls.xml.*

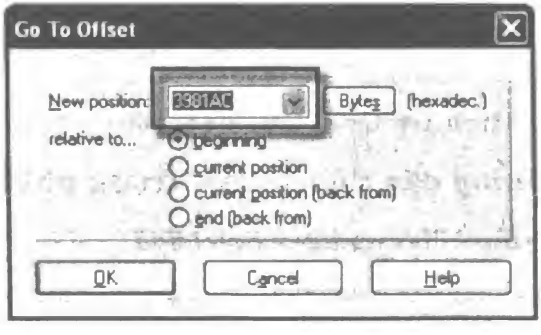
5.2. Đối với Yahoo Messenger 8.0.0.701

Với Yahoo Messenger phiên bản 8.0.0.701 hoặc cao hơn, bạn phải sử dụng một chương trình xử lý dạng số Hex như WinHex.

Bạn có thể download chương trình này tại www.minhkhai.com.vn, trong thư mục Chapter 1. Sau khi giải nén và cài đặt thành công, bạn thực hiện như sau:

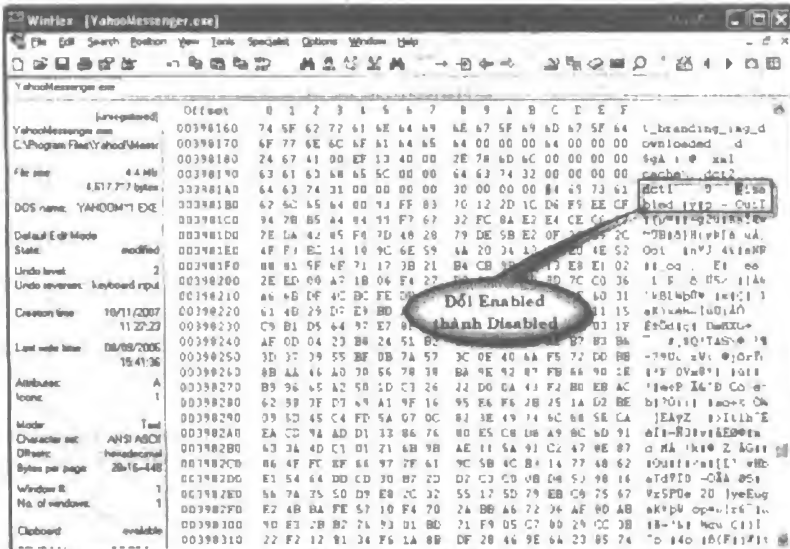
1. Vào **Start > Programs > Winhex** để mở Winhex. Tại giao diện của Winhex, vào menu **File > Open > C:\ > Program files > Yahoo! > Messenger YahooMessenger.exe**.

2. Tiếp theo, vào menu **Position > Go to Offset** hoặc nhấn tổ hợp phím **Alt + G** và nhập vào địa chỉ **3981AC**, sau đó nhấp **OK** để tìm (xem hình 1.6).



Hình 1.6: *Di chuyển đến địa chỉ 3981AC.*

3. Tiếp theo, đổi chữ **Enabled** thành **Disabled** (xem hình 1.7).



Hình 1.7: *Đổi Enabled thành Disabled.*

4. Nhấn tổ hợp phím **Ctrl + S** để lưu. Sau đó đăng nhập vào Yahoo Messenger, lúc này, mọi quảng cáo đều biến mất.

6. Chat nhiều nick với Yahoo 8.0

Khi Chat trên mạng mỗi người thường có nhiều nick name. Mỗi nick name chứa những friend list khác nhau, khi đang Chat ở nick name này và muốn chuyển sang nick name khác bạn phải thoát nick hiện hành.

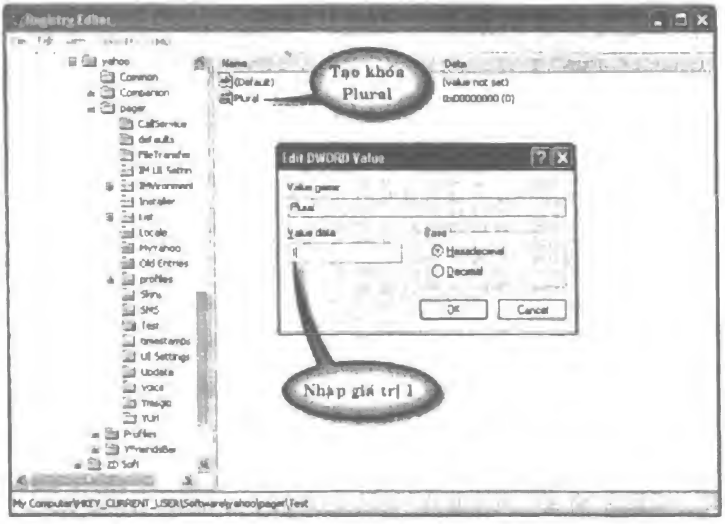
Sau đây, xin giới thiệu cùng bạn cách Chat nhiều Nick trong Yahoo Messenger phiên bản 8.0 hoặc cao hơn. Các bước thực hiện như sau:

1. Vào **Start > Run**, nhập **regedit**, sau đó nhấp **OK** để mở Registry Editor.

2. Di chuyển đến mục **HKEY_CURRENT_USER > Software > yahoo > pager > Test**.

3. Nhấp phải chuột vào ô bên phải chọn **New > DWORD value**, sau đó bạn nhập tên cho khóa này là **Plural**.

4. Nhấp đôi vào khóa **Plural** vừa tạo, nhập giá trị 1 trong mục Value Data (xem hình 1.8).



Hình 1.8: *Nhập giá trị cho khóa Plural.*

7. Loại bỏ quá trình cập nhật (Update)

Mỗi khi đăng nhập vào Yahoo Messenger, bạn phải đợi một khoảng thời gian tương đối lâu, vì Yahoo phải kiểm tra phiên bản hiện hành. Để loại bỏ tính năng kiểm tra này, bạn thực hiện như sau:

1. Vào thư mục **C:\ > Program files > Yahoo! > Messenger**.
2. Xóa tập tin **yupdater.exe** hoặc đổi tên **yupdater1.exe**. Như vậy, mỗi khi đăng nhập vào Yahoo Messenger bạn sẽ giảm được một khoảng thời gian đáng kể.

II. Bomb mail và gửi thư nặc danh

Bomb mail là phương thức mà Attacker dùng để tấn công vào Mail server nhằm làm tràn dung lượng quotas của hộp thư trên Server mail. Ngoài ra, nó còn làm cho việc kiểm tra email trở nên khó khăn và hộp mail có thể không hoạt động được nữa nếu không được xóa kịp thời.

Ngoài ra, Bomb mail còn gây nhiều thiệt hại khác như: Nội dung email chứa virus, gây ra quá trình lây nhiễm trên hệ thống, phá hủy nội dung email khác.

Phương pháp gửi Bomb mail còn được ứng dụng thông qua việc phát tán thư rác (spam mail). Biết cách hoạt động cũng như cách sử dụng một số phần mềm Bomb mail, bạn sẽ có được phương thức phòng tránh hiệu quả.

1. Mail Nuker version 1.0

Đây là chương trình Bomb mail tương đối mạnh, với Mail nuker bạn có thể gửi một lúc 1000 e-mails. Phần mềm này được phát triển bởi nhóm Outsider. Bạn có thể download chương trình này tại www.minhkhai.com.vn trong thư mục Chapter 1. Để phát tán mail bạn thực hiện theo các bước sau:

1. Trong khung Static, tại mục **Mail to**, nhập địa chỉ e-mail của người muốn gửi, ví dụ: victim@domain.com.
2. Tại mục **Mail from**, nhập địa chỉ e-mail của người gửi, tại đây bạn nhập vào e-mail bất kỳ (với mục đích ẩn danh).
3. Mục **SMTP Server**, nhập vào server mail, ví dụ smtp của các server thông dụng như:

- Yahoo: smtp.mail.yahoo.com
- Gmail: smtp.gmail.com
- Một số server mail khác: mail.domain.xxx

4. Tại mục **Subject**, nhập vào chủ đề của bức thư.
5. Tại mục **Mail Body**, nhập nội dung e-mail.
6. Mục **Number between 1- 1000**, nhập vào số lượng e-mail muốn gửi, tối đa là 1000 emails. Sau đó nhấp nút **Nuke**! để gửi cho nạn nhân (xem hình 1.9).

Hình 1.9: *Gửi bomb bằng Mail nuker.*

2. Gửi thư nặc danh bằng Ghost mail

Phần mềm này cung cấp cả mục đính kèm tập tin, bạn có thể download phần mềm này tại website www.minhkhai.com.vn.

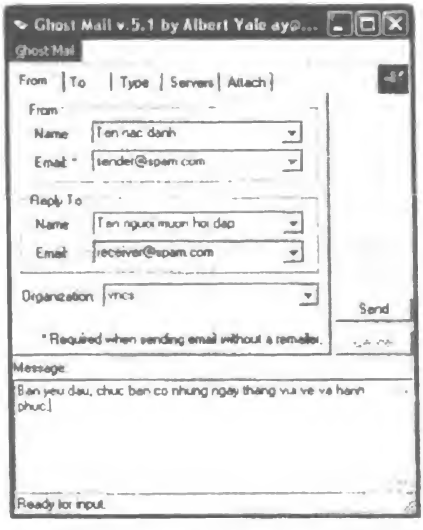
Chương trình này không cần cài đặt, sau khi giải nén, bạn thực hiện theo các bước sau:

1. Tại thẻ From, trong khung From, nhập vào các mục sau:

- **Name:** Nhập vào tên người gửi, đây là tên tùy ý.
- **E-mail:** Nhập vào địa chỉ e-mail của người gửi, địa chỉ e-mails tùy ý.

Tại mục **Reply to**, bạn nhập các mục như sau:

- **Name:** Nhập vào tên của người mà bạn muốn cho nạn nhân hồi đáp lại. Đây là tên là tùy ý.
- **E-mail:** Nhập vào e-mail mà bạn muốn nạn nhân hồi đáp vào e-mail này. Đây là địa chỉ e-mail tùy ý.
- **Organization:** Nhập vào tổ chức gửi e-mail, đây là tên tùy ý.
- **Message:** Nhập vào thông điệp muốn gửi (xem hình 1.10).



Hình 1.10: *Những thiết lập trong thẻ From.*

2. Tại thẻ **To**, bạn thiết lập các mục như sau:

- **Name:** Nhập vào tên người nhận.
- **Email:** Nhập vào địa chỉ e-mail của người nhận.
- **CC và BCC:** Gửi đến một địa chỉ e-mail khác nữa.

- **Newsgroups:** Nhập vào nhóm tin tức, nhóm này tùy ý.
- **Subject:** Nhập vào chủ đề của thư (xem hình 1.11).

Hình 1.11: *Những thiết lập trong thẻ To*

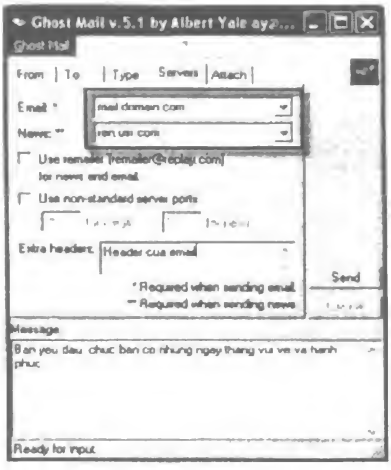
3. Tại thẻ **Type**, bạn thiết lập như sau:

Nhấp chọn vào mục **Email** và **Plain text**, các mục khác để mặc định hoặc thiết lập tùy theo ý bạn (xem hình 1.12).

Hình 1.12: *Những thiết lập trong thẻ Type.*

4. Tại thẻ **Servers**, bạn thiết lập như sau:

- **Email:** Nhập vào Mail server của nạn nhân theo cú pháp mail.domain.xxx, các mục khác để mặc định hoặc thiết lập tùy ý (xem hình 1.13).



Hình 1.13: *Những thiết lập trong thẻ Servers.*

5. Tại thẻ **Attach**, bạn thiết lập như sau:

Bạn nhấp nút **Add** để nhập vào một tập tin bất kỳ mà bạn muốn gửi, mục này hoạt động giống như mục Attach files của e-mail (xem hình 1.14).

Hình 1.14: *Những thiết lập trong thẻ Attach.*

6. Sau cùng, nhấp nút **Send** để gửi thư nặc danh cho nạn nhân.

3. Phương pháp chống thư rác và Bomb mail

Khi làm việc trong môi trường hiện đại ngày nay, ai trong chúng ta cũng ít nhiều nhận được các thư rác (spam mail). Nếu mỗi người một ngày nhận được 3 lần, mỗi lần mất 1 phút để xóa các thư rác, và mất 3 phút để

xem các chủ đề hấp dẫn do các spammer nghĩ ra thì trong một năm người đó mất 24 giờ hoặc hơn vì thư rác, bằng 3 ngày làm việc không hiệu quả. Nếu tính quy mô công ty nhỏ khoảng 30 người thì một năm mất 90 ngày công.

- **Tìm hiểu về Spam**

Spam mail là những thư điện tử gửi đến mà người dùng không mong muốn, cũng không rõ nguồn gốc của nó. Mục tiêu chính của spam không phải là làm hại người dùng, mà chỉ đơn giản làm người dùng tò mò mở thư để đọc quảng cáo một sản phẩm nào đó. Spam mail rất đa dạng và biến đổi rất nhanh, nên việc xác định ra nó không phải đơn giản. Chủ yếu đánh vào tâm lý người dùng Internet, spam mail luôn tự làm mới các chủ đề nhắm vào các lĩnh vực hấp dẫn như khuyến mãi, trúng thưởng, sex, sức khỏe,... để làm mồi nhử các nạn nhân.

- **Ai là nạn nhân của Spam mail?**

Khi bạn cung cấp địa chỉ email vào các trang web không tin cậy, email của bạn sẽ dần dần được "nổi tiếng", vì họ sẽ bán danh sách email họ có được cho các công ty khác. Nghề spam mail là nghề có thu nhập khá cao trên thế giới. Như vậy, mọi đối tượng người dùng đều rất có thể vô tình là nạn nhân của các spammer.

- **Các giải pháp loại bỏ thư rác**

Cách đơn giản nhất là sử dụng whitelist (đây là danh sách các địa chỉ email mà bạn sẵn sàng nhận). Mọi thư điện tử từ người ngoài danh sách này sẽ được đưa vào một thư mục khác để áp dụng các bộ lọc phức tạp hơn.

Một khái niệm gọi là xác nhận (challenge-respone) mở rộng phương án whitelist để ngăn các bộ máy tạo ra spam bằng cách buộc người gởi phải phản hồi chính xác. Khi nhận được 1 email từ người ngoài whitelist, hệ thống sẽ tự động trả lời email với yêu cầu nhập đúng số trong bức hình đính kèm, hoặc trả lời 1 câu hỏi. Nếu trả lời đúng, người gởi được đưa vào whitelist. Trên thực tế nó có những nhược điểm, ví dụ như làm phiền người gửi. Hơn nữa, nếu spammer mạo danh một người khác để gửi thư quảng cáo thì người bị mạo danh lại nhận được thư yêu cầu xác nhận. Nếu spammer lấy địa chỉ không có thật để mạo danh thì bạn lại nhận thêm thư "rác" thông báo "delivery failure message". Công ty MailFrontier Matador (website mailfrontier.com) cung cấp giải pháp challenge-response nhưng nhiều người dùng phải tắt tính năng này vì không hiệu quả và gây phiền toái. Hãng này phối hợp nhiều kỹ thuật để

chống spam, trong đó có whitelist, challenge-response, phân tích nội dung email và các quy tắc đặc biệt.

Cloudmark SpamNet (website cloudmark.com) sử dụng sức mạnh ý kiến của cộng đồng để lựa chọn đâu là thư rác, đâu là thư sạch. Khi xóa 1 email, bạn cũng đã gửi 1 thông điệp đến máy chủ của Cloudmark bầu chọn thư này là thư rác. Lượng khách hàng tham gia bầu chọn của SpamNet từ năm 2003 đã là 500.000 người. Nhờ vậy trong 564 thư bị từ chối chỉ có 3 thư là không phải spam mail, nhưng 55 trong số 275 thư được chấp nhận lại phải xóa bằng tay, nghĩa là có nhiều thư rác mới mà hệ thống này không nhận biết.

Ella (website openfieldsoftware.com) sử dụng kỹ thuật lọc từ các thư đã nhận. Các thư mới được chia vào 3 thư mục: Inbox, Spam, và các thư mục khác mà bạn tự định nghĩa. Sau khi phân tích khoảng 10 emails mỗi thư mục, chương trình sẽ hoàn tất bộ lọc rất ấn tượng, trong 562 thư bị đánh dấu là spam chỉ có 6 thư sạch. Nhưng thật đáng sợ là 30% thư trong inbox là rác. Sau đây xin giới thiệu một số phương pháp lọc thư rác:

Password:

Cho đối tác của bạn một mật khẩu để ghi vào chủ đề của email khi gởi cho bạn. Lọc các email không có mật khẩu trong chủ đề.

- ***Ưu điểm:*** Chỉ có ai biết mật khẩu mới gởi thư cho bạn được, spammer khó có thể có được nó.
- ***Nhược điểm:*** Thư bạn cần đọc có thể bị xóa.

Blacklist:

Khóa các thư từ những người trong danh sách cấm.

- ***Ưu điểm:*** Vô hiệu hóa các spammer đã biết, các thư không hợp lệ.
- ***Nhược điểm:*** Bỏ sót nhiều thư rác, có cả thư quảng cáo bạn muốn.

Whitelist:

Chỉ nhận thư của những người được biết.

- ***Ưu điểm:*** Khóa thư từ những nguồn không rõ.
- ***Nhược điểm:*** Khóa luôn cả những thư bạn cần nhưng chưa biết.

Challenge/Response:

Khóa các thư mà người gửi không gửi thư xác nhận.

- ***Ưu điểm:*** Vô hiệu hóa các chương trình tạo thư rác.

- ***Nhược điểm:*** Có thể khóa luôn thư bạn muốn đọc, làm phiền người gởi phải xác nhận.

Rules-Based:

Khóa thư dựa trên các quy tắc được xác định trước.

- ***Ưu điểm:*** Tìm thư rác bằng cách kiểm tra các dấu hiệu nhận biết.
- ***Nhược điểm:*** Các Spammers có thể thay đổi thư để đánh lừa hệ thống.

Community-Based:

Khóa thư dựa trên sự đồng ý của cộng đồng về thư rác.

- ***Ưu điểm:*** Nhờ một nhóm nhiều thành viên đưa ra quyết định về các email nhận được.
- ***Nhược điểm:*** Không kiểm tra được các thư mới, danh sách thư rác có thể rất dài.

Adaptive:

Học bằng cách phân tích các ví dụ mà bạn gọi là thư rác và thư sạch.

- ***Ưu điểm:*** Học từ sự lựa chọn cửa bạn, có thể phân theo mục đích riêng của từng thư mục.
- ***Nhược điểm:*** Cần thời gian để học, đặc biệt là lúc bắt đầu.

Legislative:

Sử dụng các luật đối với những thư điện tử thương mại không yêu cầu.

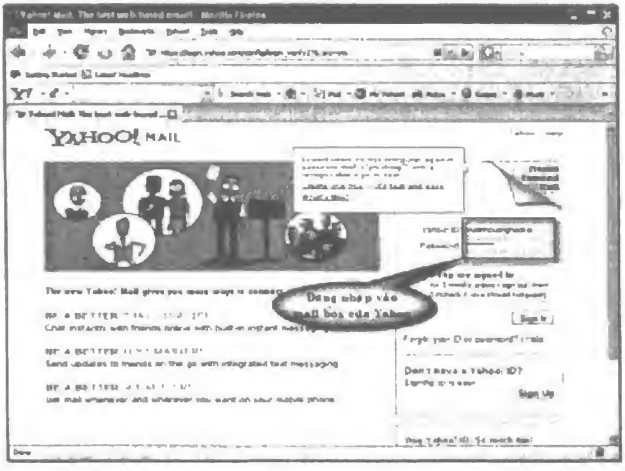
- ***Ưu điểm:*** Làm rõ các spam là bất hợp pháp, nhờ pháp luật can thiệp.
- ***Nhược điểm:*** Các spammers ở nước ngoài không bị tác động, ngoài ra có một số thư rác là hợp pháp.

- **Bomb mail và cách phòng chống**

Lọc thư dựa vào phần mở rộng:

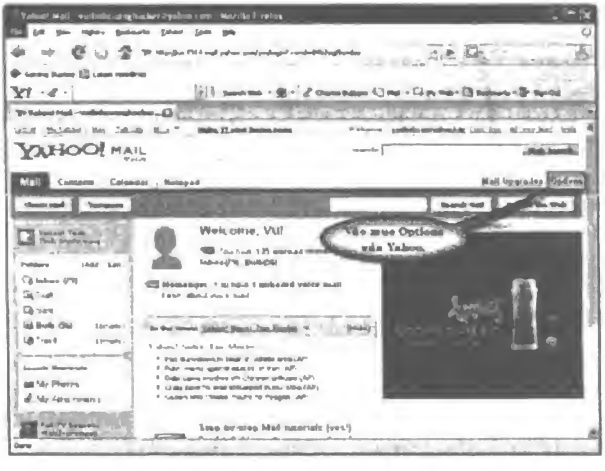
Nguyên lý của phương pháp lọc email khá đơn giản, nó dựa vào việc lọc các phần mở rộng của người gửi mail. Để thực hiện, bạn làm như sau:

1. Trên thanh Address (địa chỉ) của trình duyệt, bạn nhập **mail.yahoo.com**.
2. Nhập tên tài khoản muốn ngăn chặn Bomb mail. Ví dụ, đăng nhập với username **vudinhcuonghacker** vào Yahoo (xem hình 1.15).

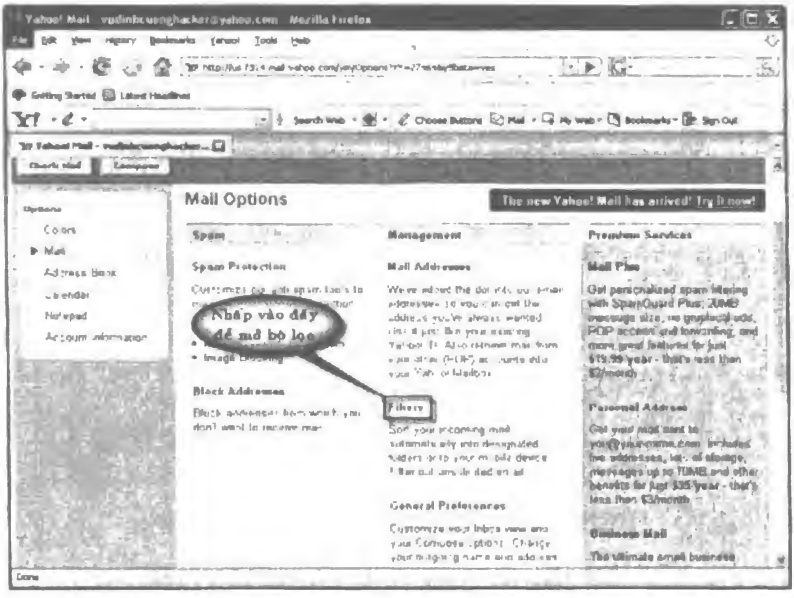


Hình 1.15: *Đăng nhập vào mail box của yahoo.*

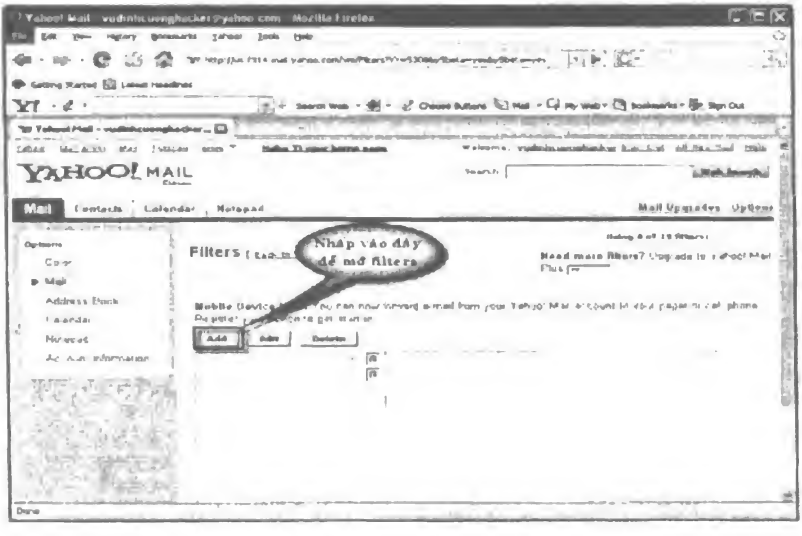
3. Nhấp nút **Options** ở phía phải bên trên cửa sổ trình duyệt để vào mục Options Yahoo (xem hình 1.16).
4. Nhấp nút **Filters** để mở bộ lọc của Yahoo. Bộ lọc này cho phép lọc nhiều thông tin liên quan đến email (xem hình 1.17).
5. Nhấp nút **Add** để mở bộ lọc (xem hình 1.18).



Hình 1.16: *Vào mục Options của Yahoo.*

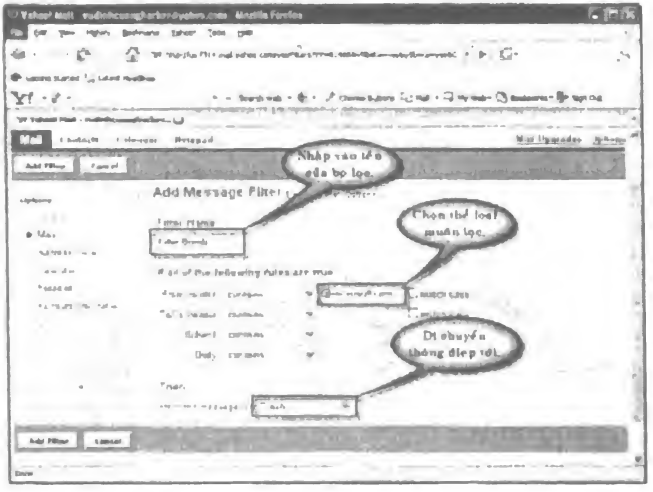


Hình 1.17: *Chọn bộ lọc của Yahoo.*



Hình 1.18: *Nhấp nút Add trong Options filters.*

6. Tại mục Filters Options, nhập tên bộ lọc trong mục Filter name, ví dụ **Filter Bomb**. Tại các mục From Header, To/cc Header, Subject, Body, bạn đều chọn là **contains**. Tiếp sau phần From Header, nhập phần mở rộng mà bạn muốn lọc, ví dụ **@microsoft.com**. Trong mục Move the message to, chọn **Trash** (xem hình 1.19).



Hình 1.19: *Những thiết lập trong bộ lọc.*

7. Nhấp nút **Add filter** để áp dụng những thiết lập.

Tới đây ta đã hoàn thành việc thiết lập bộ lọc cho những Header là @microsoft.com, bạn có thể áp dụng cách tương tự để thiết lập bộ lọc cho các chấm đuôi khác như @ftp.com, @yahoo.com, @gmail.com,...

- **Lọc thư dựa vào chủ đề (subject) và nội dung (body)**

Các website như Yahoo và Google cung cấp cho người dùng rất nhiều tiện ích miễn phí, trong đó bộ lọc thư (filter) cũng rất hay và tiện dụng. Trong mục này chúng tôi sẽ tiếp tục giới thiệu đến các bạn các phương pháp lọc thư thông qua chủ đề (subject) và nội dung (body) của bức thư.

Giả sử bạn nhận được một email như sau:

Mục From: "Nguyen Van A" nguyenvana@abc.com.

Mục To: nannhan@xyz.com.

Mục Subject: Bạn có muốn một cơ hội kiếm tiền?

Mục Nội dung:

"Xin chào! Công ty chúng tôi hiện đang muốn cộng tác với bạn, để cùng nhau kiếm tiền qua Internet.

Để xem thông tin chi tiết! xin vui lòng nhấp liên kết sau: www.abc.com".

Các bước lọc thư như sau:

1. Thực hiện từ bước 1 - 5 của mục "**Lọc thư dựa vào phần mở rộng**".
2. Tại mục Option Name nhập vào tên của bộ lọc, ví dụ, **Subject and Body**.
3. Dưới mục "If all of the following rules are true..." bạn thiết lập như sau:

   From Header: Mục này để trống.

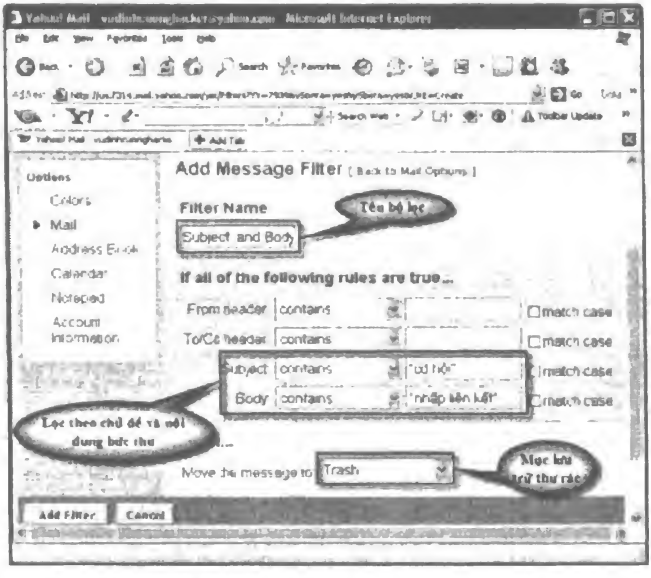
   To/Cc Header: Mục này để trống.

   Subject: Chọn **Contains**, sau đó nhập **"cơ hội"**.

   Body: Chọn **Contains**, sau đó nhập **"nhấp liên kết"**.

   Tại mục Move the message to, chọn **Trash**.

   Nhấp nút **Add Filter** để hoàn thành (xem hình 1.20).



Hình 1.20: *Lọc thư qua mục Subject và Body.*

Chú ý:

Trong mục lọc thư dựa vào chủ đề và nội dung chỉ có tính chất minh họa, bạn đọc phải phân tích kỹ chủ đề và nội dung thư để có bộ lọc tối ưu.

Ví dụ của bức thư nhận được ở trên chỉ có tính chất minh họa, hoàn toàn không ám chỉ bất kỳ một cơ quan, đơn vị nào.

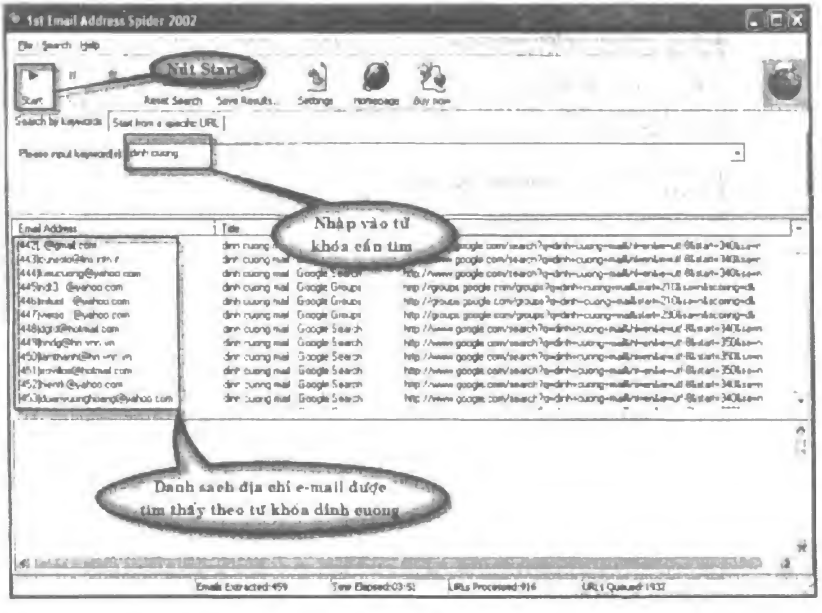
III. Các chương trình hỗ trợ E-mail

1. E-mail Spider

Để thu thập các địa chỉ emails hoặc muốn trích email trong một URL nào đó, bạn có thể sử dụng công cụ E-mail Spider, nó giúp bạn tìm kiếm nhanh chóng các địa chỉ e-mail trên các websites theo một từ khóa nhất định hoặc trích lọc địa email trong một URL cụ thể.

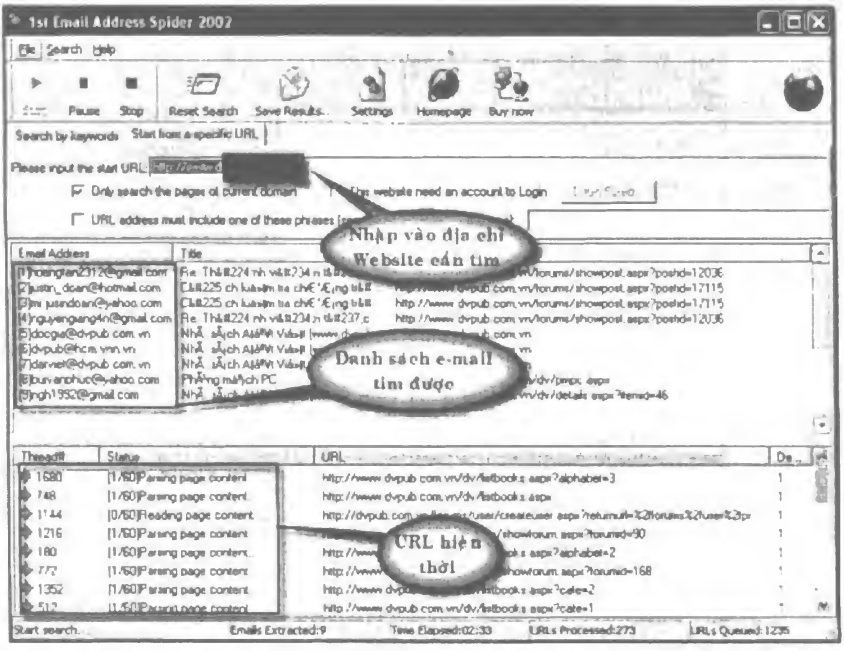
Chương trình được cung cấp tại website www.minhkhai.com.vn, thư mục Chapter 1. Sau khi giải nén và cài đặt thành công vào máy tinh, bạn thực hiện như sau:

1. Để tìm địa chỉ email theo từ khóa, tại giao diện chính của chương trình, trong mục **Please input keyword(s)**, bạn nhập vào từ khóa cần tìm. Ví dụ, nhập "**dinh cuong**", sau đó nhấp nút **Start** (xem hình 1.21).



Hình 1.21: *Tìm kiếm theo từ khóa.*

2. Tại thẻ **Start from a specific URL**, nhập địa chỉ website muốn trích lọc địa chỉ email trong mục **Please input the start URL**. Sau đó, nhấp nút **Start** để thực hiện (xem hình 1.22).



Hình 1.22: *Tìm kiếm địa chỉ e-mail theo URL.*

2. E-Mail Tracker Pro Version 7.0

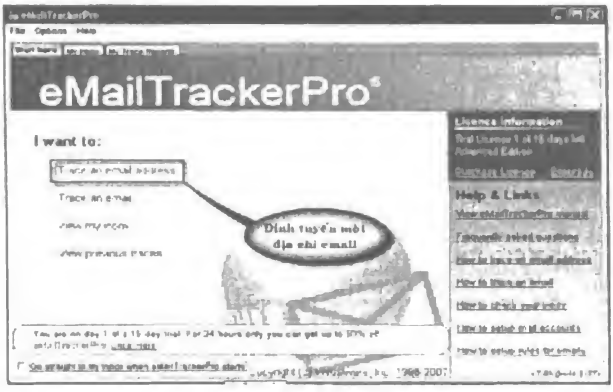
Đây là chương trình giúp bạn xác định người gửi e-mail, định tuyến và báo cáo những người phát tán thư rác. Xác định email phishing và scammer lấy thông tin mật.

Một số emails thường chứa những chương trình virus nguy hiểm và mưu đồ bất chính. Đây là nguyên nhân chính dẫn đến những thông tin mật bị mất. Với Email tracker pro bạn có thể nhanh chóng xác định được người gửi email và vị trí địa lý của những thông điệp được gửi.

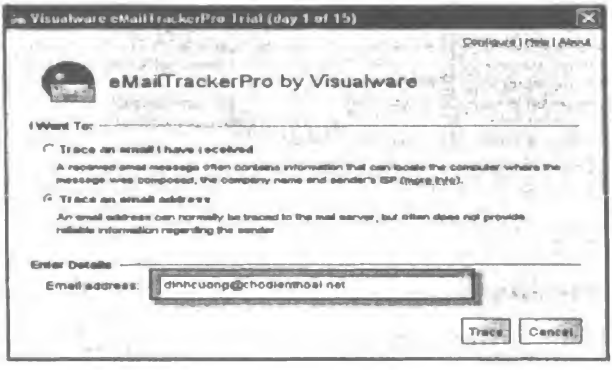
Chương trình được cung cấp tại website www.minhkhai.com.vn, thư mục Chapter 1. Sau khi giải nén và cài đặt thành công vào máy tính, bạn thực hiện như sau:

1. Trên giao diện chính của chương trình, nhấp vào mục **Trace an email Address** (xem hình 1.23).

2. Tại **Email Address**, nhập vào địa chỉ email muốn tìm thông tin. Ví dụ: **dinhcuong@chodienthoai.net**, tiếp theo nhấp nút **Trace** để thực hiện (xem hình 1.24).

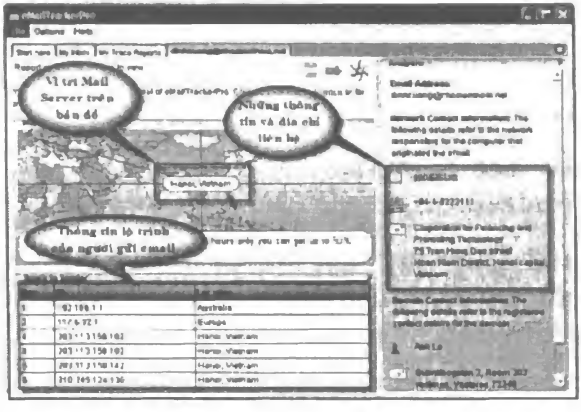


Hình 1.23: *Định tuyến một địa chỉ email.*



Hình 1.24: *Nhập vào địa chỉ email.*

3. Sau khi nhấp nút Trace, bạn đợi khoảng 30 giây chương trình sẽ thống kê những thông tin như: Vị trí địa lý của người gửi email, mail server, tên admin và địa chỉ liên hệ của domain,.. (xem hình 1.25).



Hình 1.25: *Những thông tin thống kê được.*

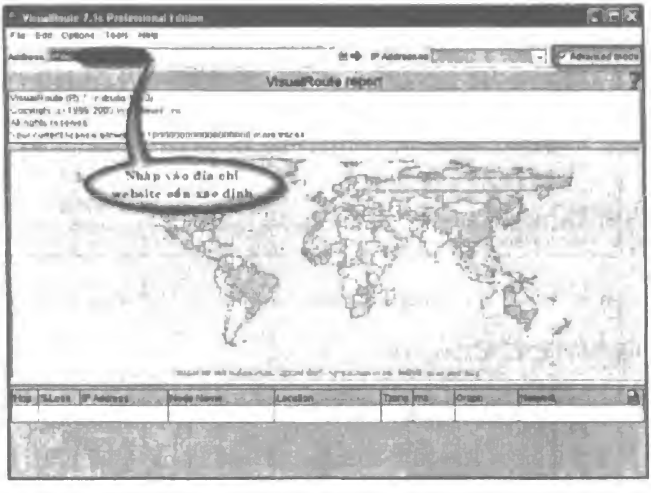
3. Visual Route Version 7.1

Chương trình cho phép thực hiện các lệnh Ping, Whois và Traceroute. Nó có khả năng tự động phân tích các vấn đề kết nối, hiển thị các kết quả trên bản đồ thế giới, đây là công cụ tốt nhất để định vị và xác định những người lừa đảo trên Internet.

Chương trình được cung cấp tại website www.minhkhai.com.vn, thư mục Chapter 1. Sau khi giải nén và cài đặt thành công vào máy tính, bạn thực hiện như sau:

3.1. Xác định vị trí địa lý của Web site

1. Trên thanh Address (địa chỉ) của chương trình, nhập vào địa chỉ website muốn xác định, ví dụ như www.microsoft.com, tiếp theo nhấn **Enter** để thực hiện (xem hình 1.26).

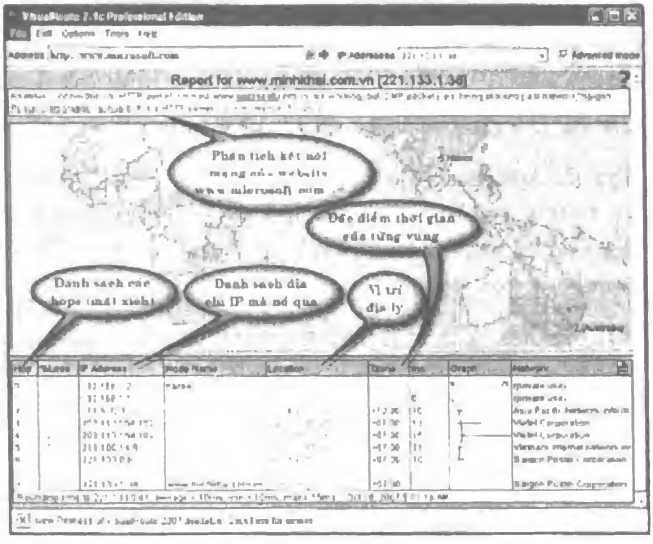


Hình 1.26: *Nhập thông tin cần tìm.*

2. Sau khi nhấn **Enter**, đợi chương trình xử lý khoảng 30 giây, nó cho ta những thông tin sau:

- Gần trên thanh Address của chương trình cho chúng ta một bản phân tích về tình trạng kết nối của trang www.microsoft.com như: Các kết nối đến HTTP ở cổng 80 đến host www.microsoft.com đang hoạt động, nhưng gói ICMP bị khóa khi qua mạng của cong ty Saigon Postel Corporations ở hop 6, HTTP Server đang chạy Microsoft IIS/6.0.
- Chương trình cùng hiển thị cho chúng ta thấy các kết nối thông qua bản đồ thế giới

- Visual route còn cho chúng ta biết những thống kê chi tiết về quá trình chuyển tải của mạng thông qua các hop được tính từ địa chỉ IP của máy chúng ta đến http Server.
- Chương trình cũng thống kê địa chỉ IP của các hosts trung gian, vị trí địa lý của các hosts này, thời gian của vùng và hệ thống mạng của từng kết nối (xem hình 1.27).

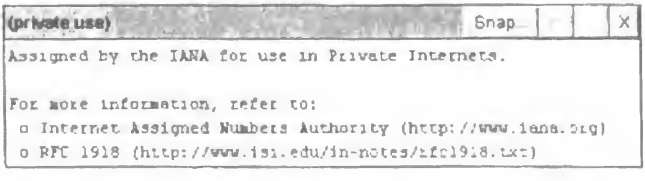


Hình 1.27: *Những thông tin mà chương trình thống kê được.*

3.2. Những thông tin mạng

1. Thông tin thống kê của địa chỉ IP 192.168.1.2

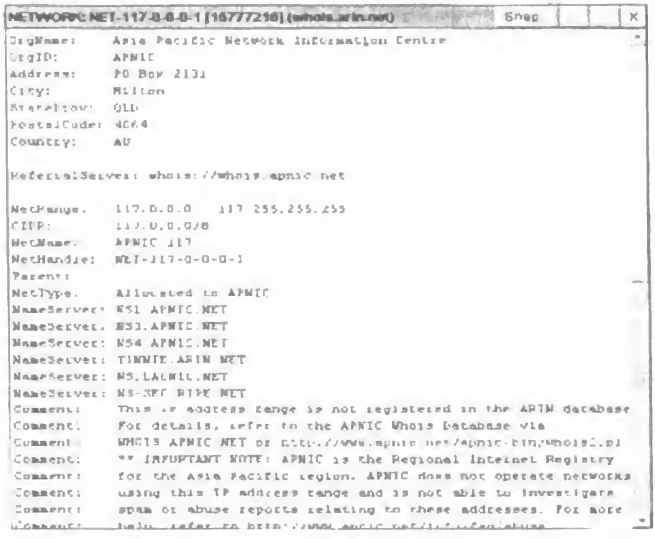
Trong bảng thống kê của chương trình cũng cho biết những thông tin của từng mạng theo từng địa chỉ IP cụ thể mà nó đi qua. Ví dụ, từ địa chỉ IP 192.168.1.2, nhấp vào mục Private use, bạn nhận được thông tin thống kê như trong hình 1.28.



Hình 1.28: *Thông tin thống kê của IP 192.168.1.2.*

2. Những thông tin thống kê của địa chỉ IP 17.6.32.1

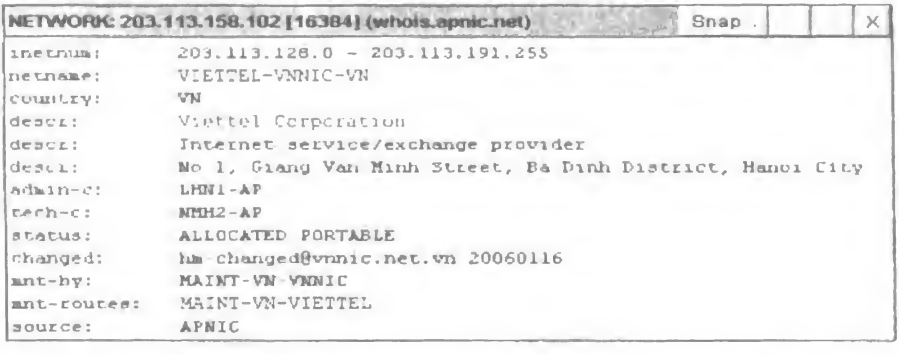
Đây là một host của Australia, để có những thông tin này bạn nhấp vào mục **Asia pacific network inform** (xem hình 1.29).



Hình 1.29: *Thông tin của IP 17.6.32.1.*

3. Những thông tin của mạng Viettel Corporation

Tại mục này bạn nhấp vào mục **Viettel Corporation** có địa chỉ IP là 203.113.158.102, đây là host có Server ở Hà Nội – Việt Nam (xem hình 1.30).

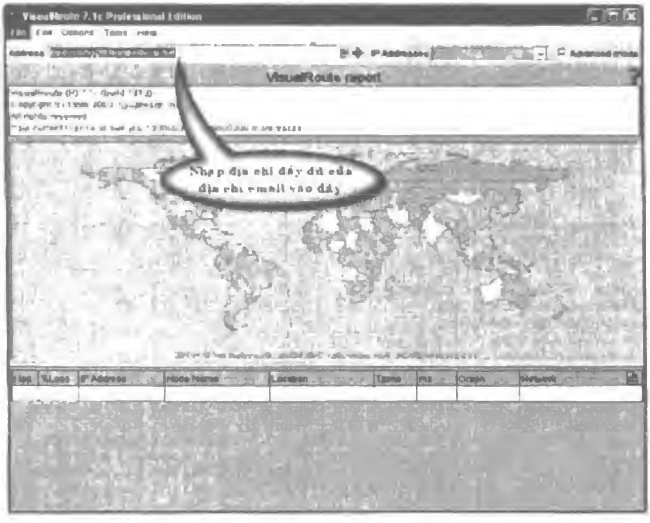


Hình 1.30: *Những thông tin của Viettel Corporation.*

3.3. Xác định địa chỉ E-mail

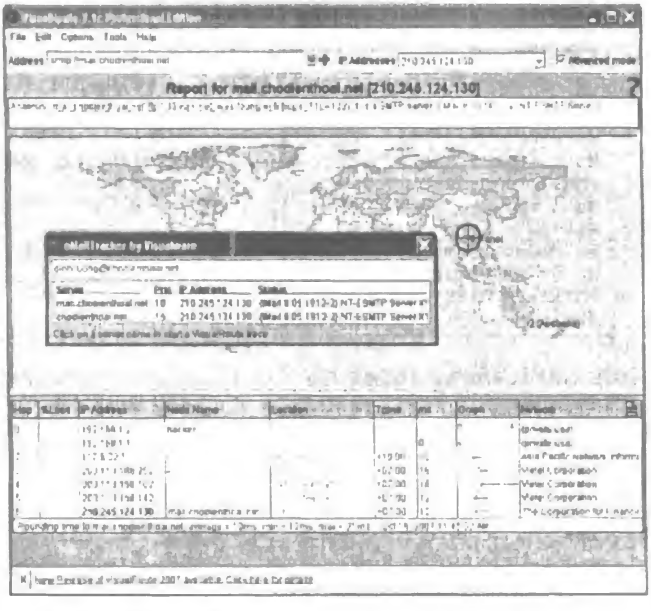
Để xác định các thông tin của một email cụ thể nào đó, bạn làm như sau:

1. Trên thanh Address của chương trình, nhập địa chỉ email muốn xác định. Ví dụ như dinhcuong@chodienthoai.net, sau đó nhấn **Enter** để thực hiện (xem hình 1.31).



Hình 1.31: *Nhập địa chỉ email.*

2. Sau khi quá trình xác định hoàn thiện, bạn nhấp vào Mail server muốn xem, ví dụ là **mail.chodienthoai.net**, chương trình sẽ thống kê cho chúng ta những thông tin như: Vị trí địa lý của email, địa chỉ IP của mail server, và những thông tin thống kê về mạng (xem hình 1.32).



Hình 1.32: *Những thông tin thống kê được.*

Chương 2:

TÌM LẠI PASSWORD WINDOWS

- **Tìm hiểu về Password.**
- **Sao chép tập tin hệ thống bằng chương trình Volkov Commander 4.99.**
- **Active Password Changer 3.0.0.420 (NT/2000/XP/2003/Vista).**
- **Windows Password Cracker V. 2.1.9.0.**
- **Advanced Windows Password Recovery 2.9.2.224.**
- **L0pCrack 5.02.**
- **Proactive Windows Security Explorer™.**
- **Xem password đằng sau dấu sao (*).**

Từ khi Windows 2000 Professional ra đời, hệ điều hành đã trở nên bảo mật hơn. Password đăng nhập được cải thiện đáng kể. Do vậy khi vào máy tính, không thể nào nhấp nút Cancel như Windows 9x mà bạn phải chứng thực đăng nhập bằng username và password hợp lệ.

Microsoft sử dụng nhiều thuật toán phức tạp để mã hóa dữ liệu nhập, nhằm tạo ra độ phức tạp cao cho chuỗi password. Tuy nhiên, ta hãy xem xét password đăng nhập ở một vài khía cạnh khác như: Khi cơ quan thay đổi nhân sự, password đăng nhập vào hệ điều hành chưa được bàn giao, cha mẹ muốn kiểm tra máy tính của con mình nhưng không thể vào được hệ điều hành, khi quản lý mạng và cung cấp một số lượng tài khoản lớn thì việc quên password là một điều không thể tránh khỏi,...

Chương này giới thiệu đến bạn các phương pháp tìm lại password Windows và cách sử dụng một số phần mềm chuyên dụng như: Active Password Changer, L0pCrack,... Đây là những chương trình giúp nhanh chóng loại bỏ và tìm lại password Windows.

Đọc và thực hiện theo những hướng dẫn của chương, bạn hoàn toàn làm chủ được quá trình đăng nhập vào Windows dưới mọi hình thức.

I. Tìm hiểu về password

1. Các loại password

Để có những password đủ mạnh và hiệu quả, trước tiên ta phải tìm hiểu về các loại password sau:

- Password chỉ chứa những ký tự in hoa, ví dụ: VNCS.
- Password chỉ chứa các ký tự số, ví dụ: 12548736.
- Password chỉ chứa các ký tự đặc biệt, ví dụ: $@$!().
- Password chứa các ký tự và ký tự số, ví dụ: vncs12548.
- Password chỉ chứa các ký tự và ký đặc biệt, ví dụ: cd@ro$.
- Password chỉ chứa các ký tự đặc biệt và ký tự số, ví dụ: @#12.
- Password chứa ký tự, ký tự đặc biệt và ký tự số, ví dụ: NHg@12.

Một password mạnh thì nó phải được kết hợp ký tự hoa, ký tự thường, ký tự số, ký tự đặc biệt và độ dài của password phải lớn hơn 8. Ngoài ra, bạn phải kết hợp cả ký tự khoảng trắng trong chuỗi password.

2. Tìm hiểu về Shadow Password

Trước đây, Unix không sử dụng kỹ thuật Shadow Password. Từ phiên bản System V Release 3.2 (1987), BSD4.3 Reno (1991) và Linux (1992) mới ứng dụng kỹ thuật Shadow. Các phiên bản Unix khác nhau đều có cùng nguyên tắc xử lý Shadow. Chỉ có điểm khác biệt là tên gọi tập tin Shadow và vị trí chứa tập tin này khác nhau trên các Unix khác nhau. Ví dụ, trên Linux, Shadow nằm ở /etc/shadow, trên BSD, Shadow ở vị trí /etc/master.passwd, trên HP-UX thì Shadow nằm tại /.secure/etc/passwd,... Có một số Unix tạo Shadow riêng cho từng username.

Về cách "mã hoá" Shadow thì tổng thể như sau: khi user được cung cấp một pasword hoặc anh ta chọn một password, password này được mã hóa (encoded) với giá trị ngẫu nhiên được gọi là salt. Giá trị salt được lưu cùng với password đã được mã hóa (encoded) trên hệ thống.

Khi người dùng đăng nhập (login) bằng password của mình, giá trị salt được lấy ra từ password đã mã hóa và được lưu trên hệ thống, giá trị salt dùng để mã hóa (encode password) mà người dùng vừa nhập vào. Nếu hai giá trị: password đã lưu và password vừa được mã hóa (mã hóa bằng từ khóa salt) trùng nhau thì người dùng được xác thực.

Quy trình mã hóa ở đây gọi là "one way hash function". Hàm crypt() được sử dụng để thực thi (bạn có thể tìm hiểu về hàm crypt bằng cách nhập **man crypt**). Một số điểm quan trọng của hàm crypt() như sau:

- Hàm Crypt(): Dùng để "mã hoá" mật khẩu, dựa trên tiêu chuẩn thuật toán DES.
- Khóa (key): Là giá trị password (ở dạng chuỗi) mà người dùng nhập vào.
- Salt: Là chuỗi có 2 ký tự được chọn từ chuỗi [a-z], [A-Z], [0-9], [./] (các ký tự từ a đến z cho chữ thường và chữ in, các ký tự số từ 0 đến 9, thêm vào đó là 2 ký tự . và /). Từ chuỗi này mới tạo ra giá trị ngẫu nhiên từ 4096 khả năng khác nhau.
- Các ứng dụng mở rộng trên các thư viện dùng cho hàm này có chức năng dùng các thuật toán khác thay vì DES có thể tạo chuỗi hash lớn hơn.

Hướng dẫn thêm:

- **Shadowed password**: Là quá trình bao gồm salt (để mã hóa password khi user nhập password vào) và chuỗi được mã hóa (encoded string) (dùng để so sánh với giá trị vừa nhập vào và đã được mã hóa). Gọi chung đây là "Hash".
- **DES (Data Encryption Standard, hay Tiêu chuẩn Mã hóa Dữ liệu)** là một phương pháp mã hóa mật được FIPS (Tiêu chuẩn xử lý thông tin Liên bang Hoa Kỳ) chọn làm chuẩn chính thức vào năm 1976. Sau đó chuẩn này được sử dụng rộng rãi trên phạm vi thế giới. Ngay từ đầu, thuật toán của nó đã gây ra rất nhiều tranh cãi, do nó bao gồm các thành phần thiết kế mật, độ dài khóa tương đối ngắn, và các nghi ngờ về cửa sau để Cơ quan An ninh Quốc gia Hoa Kỳ (NSA) có thể bẻ khóa. Do đó, DES đã được giới nghiên cứu xem xét rất kỹ lưỡng, việc này đã thúc đẩy hiểu biết hiện đại về mật mã khối (block cipher) và các phương pháp thám mã tương ứng.

Hiện nay, DES được xem là không đủ an toàn cho nhiều ứng dụng. Nguyên nhân chủ yếu là độ dài 56 bit của khóa là quá nhỏ. Khóa DES đã từng bị phá trong vòng chưa đầy 24 giờ. Đã có rất nhiều kết quả phân tích cho thấy những điểm yếu về mặt lý thuyết của mã hóa có thể dẫn đến phá khóa, tuy chúng không khả thi trong thực tiễn. Thuật toán được tin tưởng là an toàn trong thực tiễn có dạng Triple DES (thực hiện DES ba lần), mặc dù trên lý thuyết phương pháp này vẫn có thể bị phá. Gần

đây, DES đã được thay thế bằng AES (*Advanced Encryption Standard*, hay Tiêu chuẩn mã hóa tiên tiến).

Trong một số tài liệu, người ta phân biệt giữa DES (là một tiêu chuẩn) và thuật toán **DEA** (*Data Encryption Algorithm*, hay Thuật toán Mã hóa Dữ liệu) - thuật toán dùng trong chuẩn DES.

- **AES (Advanced Encryption Standard**, hay **Tiêu chuẩn mã hóa tiên tiến**) là một thuật toán mã hóa khối. Giống như tiêu chuẩn DES, AES được kỳ vọng áp dụng trên phạm vi thế giới và đã được nghiên cứu rất kỹ lưỡng. Thuật toán được thiết kế bởi hai nhà mật mã học người Bỉ: Joan Daemen và Vincent Rijmen lấy tên chung là "Rijndael" khi tham gia cuộc thi thiết kế AES.

- **Mô tả thuật toán DES**

DES là thuật toán mã hóa khối, nó xử lý từng khối thông tin của bản rõ (bản chứa các ký tự do người dùng nhập vào và chưa được mã hóa) có độ dài xác định và biến đổi theo những quá trình phức tạp để trở thành khối thông tin của bản mã (bản chứa các thông tin được mã hóa) có độ dài không thay đổi. Trong trường hợp của DES, độ dài mỗi khối là 64 bit. DES cũng sử dụng khóa (một chuỗi ký tự dùng để mã hóa và giải mã) để cá biệt hóa quá trình chuyển đổi. Nhờ vậy, chỉ khi biết khóa mới có thể giải mã được văn bản mã. Khóa dùng trong DES có độ dài toàn bộ là 64 bit. Nhưng chỉ có 56 bit thực sự được sử dụng, 8 bit còn lại chỉ dùng cho việc kiểm tra. Vì thế, độ dài thực tế của khóa chỉ là 56 bit.

3. Password Windows

Password Windows là phương pháp bảo mật tài khoản người dùng trong quá trình đăng nhập. Để tìm hiểu về password Windows, trước tiên ta phải biết vị trí lưu trữ của password trong máy tính.

Password Windows được lưu trong thư mục Windows\System32\Config\. Những files chứa password có thể là SAM hoặc _SAM, tùy thuộc vào phiên bản của hệ điều hành. Như vậy, nếu file password của Windows là SAM thì đường dẫn đầy đủ của file password là C:\Windows\System32\Config\SAM. Trong đó C:\ là ổ đĩa ta cài đặt hệ điều hành Windows.

Một số tập tin liên quan đến tài khoản, đặc quyền của người dùng như: SYSTEM, SECURITY cũng nằm trong thư mục Config.

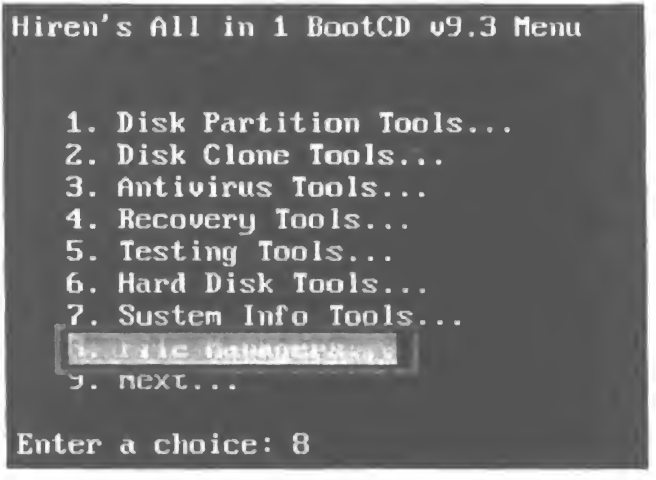
II. Sao chép tập tin hệ thống bằng chương trình Volkov Commander 4.99

Các tập tin hệ thống trong thư mục Config luôn được bảo vệ ở các chế độ đặc biệt. Do vậy, không thể sao chép các tập tin này ngay trong môi trường Windows, không thể truy cập nó bằng những thao tác mở file thông thường. Muốn lấy được những tập tin này, bạn phải có giải pháp phù hợp.

Trong mục này giới thiệu một phương pháp đơn giản để sao chép các tập tin hệ thống bằng chương trình Volkov Commander 4.99 và NTFS DOS Pro 5.0. Hai phần mềm này đều có trong đĩa Hirent's boot, bạn có thể download tại website www.minhkhai.com.vn, thư mục Chapter 2.

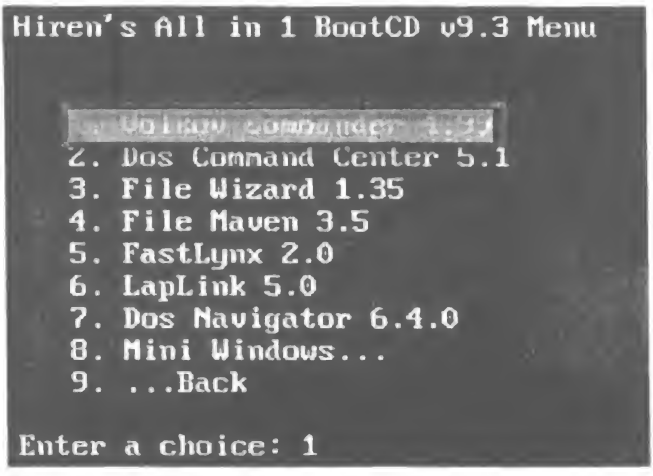
Chương trình hoạt động tương tự như Norton Commander, nhưng mạnh hơn nhiều bởi nó đã hỗ trợ truy cập vào cả những phân vùng NTFS. Để thực hiện bạn làm như sau:

1. Thiết lập trong BIOS cho phép khởi động máy tính bằng CD-ROM. Tiếp theo, khởi động máy tính bằng Hirent's Boot CD 9.3.
2. Tại giao diện chính của Hirent's Boot CD 9.3, di chuyển thanh sáng đến menu **File Managers**, sau đó nhấn **Enter** để tiếp tục (xem hình 2.1).



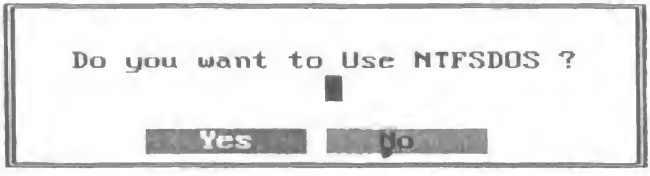
Hình 2.1: *Chọn File Managers.*

3. Di chuyển thanh sáng đến menu **Volkov Commander 4.99**, sau đó nhấn **Enter** để nạp chương trình (xem hình 2.2).



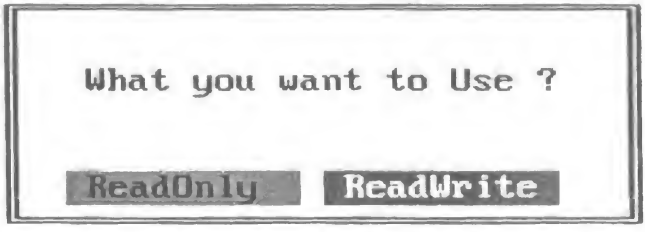
Hình 2.2: *Chọn Volkov Commander.*

4. Đợi khoảng 1 phút, chương trình giải nén các tập tin cần thiết lên RAM. Tiếp theo, chương trình hỏi: "**Do you want to use NTFSDOS ?**" (Bạn có muốn sử dụng NTFSDOS không ?). Nếu đĩa cứng được phân vùng là NTFS thì bạn chọn **Yes**, sau đó nhấn **Enter** để tiếp tục (xem hình 2.3).



Hình 2.3: *Sử dụng NTFSDOS.*

5. Chương trình sẽ hỏi: "**Do you want to use ?**". Chọn **ReadWrite**, sau đó nhấn **Enter** để áp dụng (xem hình 2.4).



Hình 2.4: *Chọn ReadWrite.*

Lựa chọn này cho phép đọc ghi trên môi trường DOS NTFS.

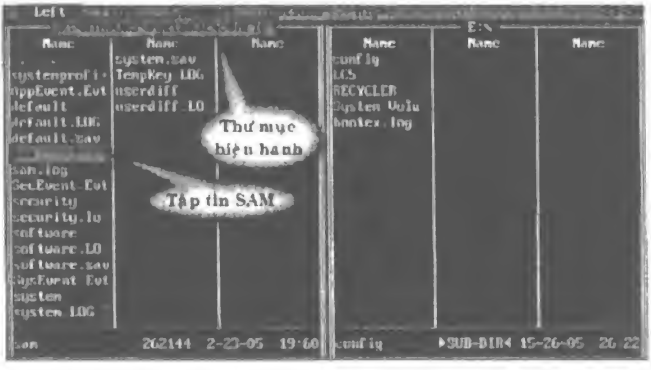
6. Nhấn tổ hợp phim **Alt + F1** để chọn ổ đĩa cần mở cho cửa sổ trái. Trong danh sách các ổ đĩa, chọn ổ đĩa **D** (xem hình 2.5).

Hình 2.5: *Chọn ổ đĩa D cho cửa sổ bên trái.*

Ổ đĩa C trong môi trường DOS đã trở thành ổ đĩa D.

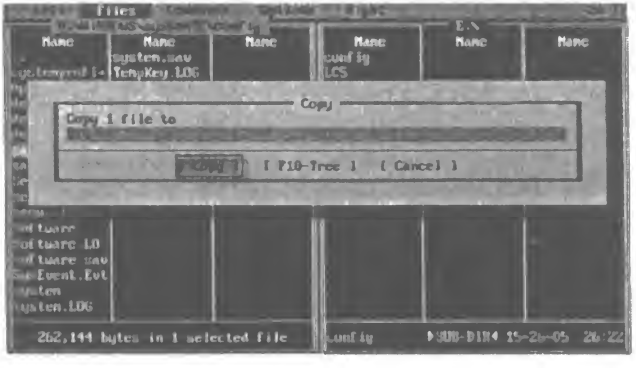
7. Nhấn tổ hợp phím **Atl + F2** để chọn ổ đĩa cần mở cho cửa sổ phải, bạn chọn ổ đĩa **E**.

8. Tiếp theo, nhấn phím **Tab** để di chuyển thanh sáng sang cửa sổ bên trái, tiếp theo chỉ chuyển đến thư mục **Windows** và nhấn **Enter**. Sau đó, tiếp tục di chuyển đến thư mục **System32** và **Config**, nhấn **Enter** (xem hình 2.6).



Hình 2.6: *Giao diện của Volkov Commander.*

9. Di chuyển thanh sáng đến tập tin SAM, tiếp theo nhấn phím **Insert** để chọn, sau đó nhấn phím **F5** và nhấn **Enter** để copy file SAM sang thư mục gốc của ổ đĩa E (xem hình 2.7).



Hình 2.7: *Copy tập tin Sam sang ổ đĩa E.*

10. Sau khi copy xong, bạn khởi động lại máy tính và bây giờ, bạn đã có file SAM được lưu trữ trong ổ đĩa **D** (tức là ổ đĩa E trong MS DOS).

Bạn áp dụng cách tương tự để sao chép các tập tin SYSTEM, SECURITY trong thư mục config. Khi có được tập tin SAM, bạn có thể sử dụng chương trình L0pCrack 5.02 hay bất kỳ một chương trình dò tìm password Windows nào để tìm password (xem mục IV).

III. Active Password Changer 3.0.0.420 (NT/2000/XP/2003/Vista)

Chương trình này giúp bạn nhanh chóng loại bỏ password đăng nhập trong tất cả các phiên bản của Windows như: Windows NT/2000/XP/2003 và hệ điều hành Windows Vista. Phương thức hoạt động của nó là thay thế password của một tài khoản được chỉ định bằng ký tự NULL. Do vậy, khi ta đã loại bỏ password thì khi đăng nhập sẽ không phải nhập bất kỳ một ký tự nào.

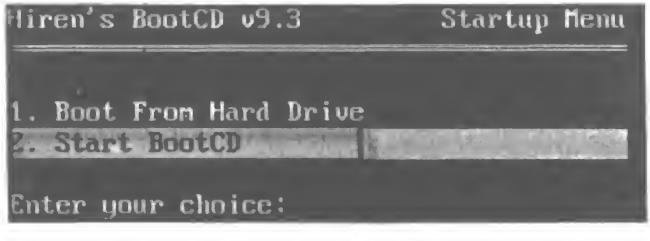
Phần mềm này có trong đĩa Hirent's Boot CD 9.3, được cung cấp tại website www.minhkhai.com.vn, thư mục Chapter 2. Trong mục này sẽ loại bỏ password tài khoản administrator tại thư mục Windows được tạo tại ổ đĩa C của máy tính cục bộ. Các bước thực hiện như sau:

1. Chọn chế độ khởi động trong BIOS là CD-ROM.

Bạn sử dụng Hirent's Boot CD 9.3 được cung cấp dưới dạng file .iso, sau đó dùng Nero burn để ghi thành đĩa Boot. Tiếp theo, thiết lập trong Bios để cho khởi động từ đĩa này.

2. Tiếp theo, khởi động lại máy tính và di chuyển thanh sáng xuống menu **Start bootCD**.

Khi quá trình boot từ CD-ROM được bắt đầu, chương trình trong Hirent's Boot CD cho 2 lựa chọn. Bạn có thể tiếp tục khởi động vào Windows bằng cách chọn Boot From Hard Drive hoặc boot từ đĩa CD bằng cách chọn Start bootCD (xem hình 2.8).



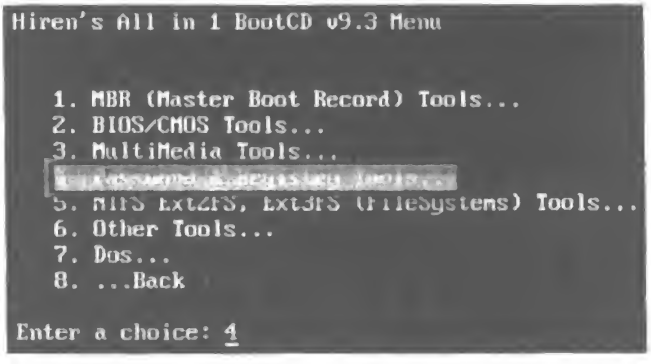
Hình 2.8: *Chọn Start BootCD.*

3. Di chuyển thanh sáng xuống menu **Next** và nhấn **Enter** để tiếp tục (xem hình 2.9).

4. Di chuyển thanh sáng đến menu **Password & Registry Tools** và nhấn **Enter** để mở menu này.

Trong menu này chứa rất nhiều công cụ liên quan đến Password và công cụ soạn thảo registry (xem hình 2.10).

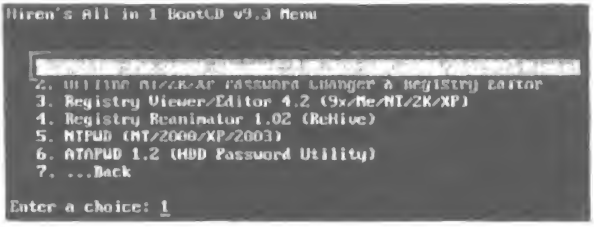
Hình 2.9: *Chọn menu Next.*



Hình 2.10: *Chọn Password & Registry Tools.*

5. Di chuyển thanh sáng đến menu **Active Password Changer 3.0.420 (2000/XP/2003/Vista)** và nhấn **Enter** (xem hình 2.11).

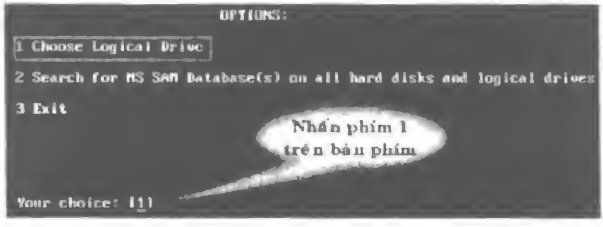
6. Chương trình giải nén các tập tin của chương trình lên RAM của máy tính. Sau khi giải nén xong, chương trình được nạp và hiển thị. Tại giao diện này bạn chọn **Choose Logical Drive** bằng cách nhấn phím số **1** trên bàn phím sau đó nhấn **Enter** để tiếp tục.



Hình 2.11: *Chọn Active Password Changer 3.0*

Các lựa chọn của mục này như sau:

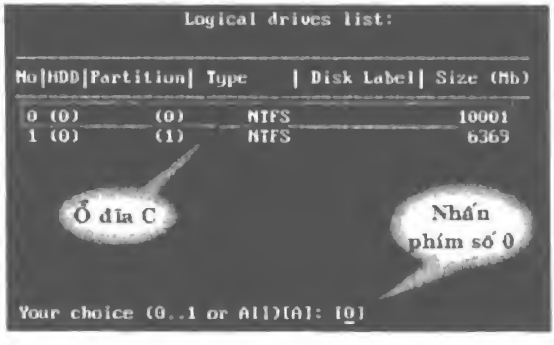
- **Choose Local Drive:** Chọn ổ đĩa chứa hệ điều hành. Nếu bạn biết rõ hệ điều hành được cài vào phân vùng nào trên đĩa cứng thì bạn có thể chọn mục này.
- **Search for MS SAM Database(s) on all hard disks and logical drives**: Tự động tìm tập tin SAM trên tất cả các đĩa cứng của máy tính.
- **Exit:** Thoát chương trình (xem hình 2.12).



Hình 2.12: *Chọn Choose Logical Drive.*

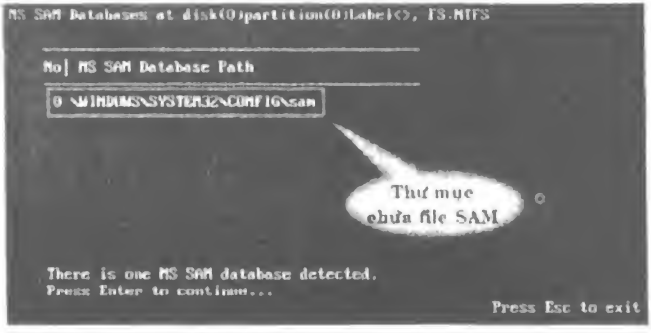
7. Nhấn phím số **0** trên bàn phím để chọn ổ đĩa C.

Danh sách ổ đĩa bắt đầu từ 0, trong mục này máy tính của chúng ta có 2 ổ đĩa, do vậy chương trình sẽ liệt danh sách bao gồm 0 và 1 (xem hình 2.13).



Hình 2.13: *Chọn ổ đĩa C.*

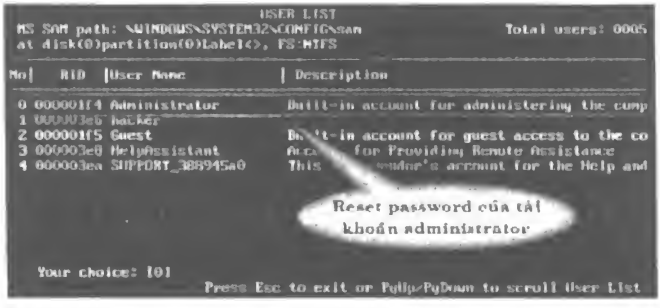
8. Đợi một lúc để chương trình tìm tập tin **SAM** trong phân vùng C. Sau đó, chương trình hiển thị đường dẫn chứa tập tin SAM trong máy tính (xem hình 2.14)



Hình 2.14: *Tập tin SAM trên máy tính.*

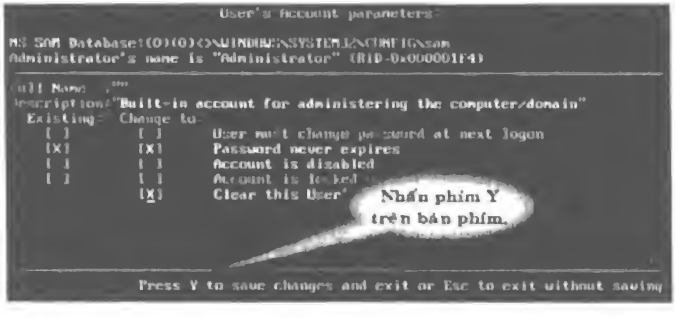
9. Chọn tài khoản **Administrator** bằng cách nhấn phím **0** trên bàn phím, sau đó nhấn **Enter** để thực hiện.

Các tài khoản được liệt kê theo thứ tự từ 0 (xem hình 2.15).



Hình 2.15: *Loại bỏ password Administrator.*

10. Những thiết lập khác để mặc định, nhấn phím **Y** trên bàn phím để thực hiện loại bỏ password (xem hình 2.16).



Hình 2.16: *Nhấn phím Y.*

11. Tiếp theo, bạn khởi động lại máy tính và cho hệ thống khởi động từ Hard disk, đăng nhập vào tài khoản administrator.

Hướng dẫn thêm:

- Bạn có thể áp dụng cách trên để loại bỏ password của các tài khoản khác nhau. Để quay lại các bước trước, sau khi kết thúc ở bước 10, bạn chỉ cần nhấn phím Esc.
- **Loại bỏ password:** Là quá trình thay thế password của tài khoản người dùng bằng ký tự rỗng (NULL). Cách này chỉ áp dụng khi người dùng quên password mà thôi. Vì khi loại bỏ password thì người dùng không thể đăng nhập vào hệ thống bằng password cũ được nên sẽ để lại dấu vết.
- **Tìm lại password:** Là quá trình sử dụng các chương trình để tìm ra chính xác password của tài khoản người dùng. Các chương trình dò tìm password sẽ sử dụng các thuật toán được lập trình sẵn để tìm lại password của tài khoản được chỉ định hay tất cả các tài khoản trong Windows. Phương pháp mà các chương trình dò tìm password thường áp dụng là Brute-Force (thử sai) và Dictionary (từ điển).

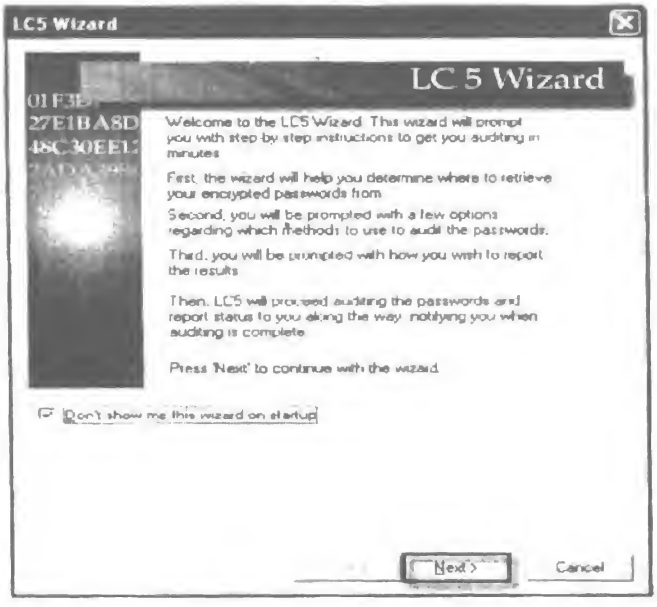
IV. L0pCrack 5.02

Chương trình này giúp tìm lại password Windows và UNIX. Ngoài chức năng giải mã password trên máy tính cục bộ, chương trình còn cho phép tìm lại password Windows/Unix trong mạng LAN, hay từ một project đã được lưu.

Chương trình được cung cấp tại website www.minhkhai.com.vn, thư mục Chapter 2. Sau khi giải nén và cài đặt thành công chương trình vào máy tính, bạn thực hiện như sau:

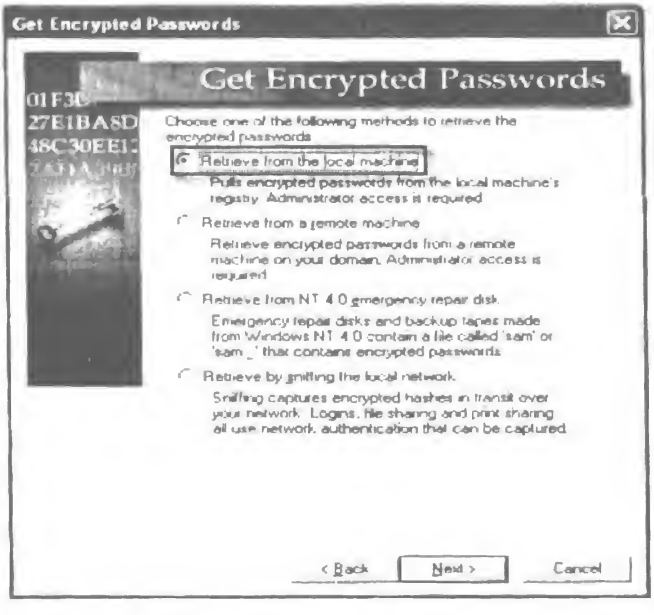
1. Tìm lại password Windows trên máy tính cục bộ

1. Vào **Start > Programs > LC5 > LC5** để khởi động chương trình (xem hình 2.17).
2. Nhấp **Next**, tiếp theo nhấp chọn vào mục **Retrieve from the local machine**, sau đó nhấp **Next** để tiếp tục.



Hình 2.17: *Giao diện của LC5 Wizard.*

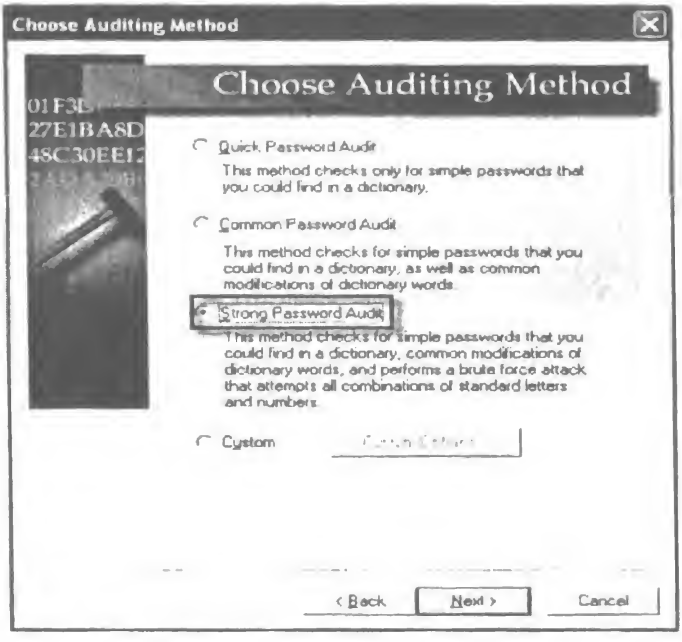
Lựa chọn này cho phép tìm kiếm các tài khoản trong máy tính cục bộ (xem hình 2.18).



Hình 2.18: *Chọn Retrieve from the local machine.*

3. Nhấp chọn vào **Strong Password Audit**.

Lựa chọn này có chức năng tìm nhanh các password đơn bằng phương pháp Brute-force (thử sai) (xem hình 2.19).



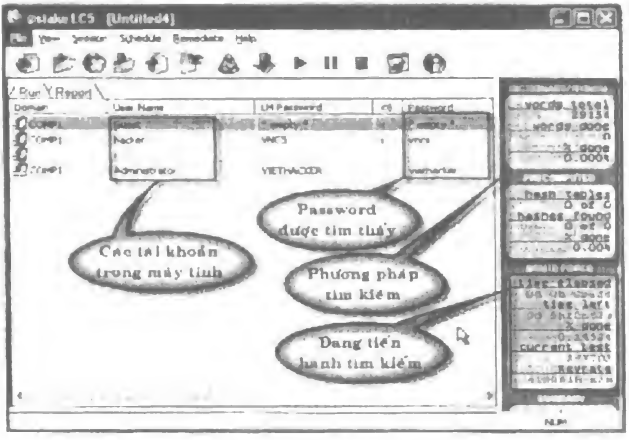
Hình 2.19: *Chọn Strong Password Audit.*

4. Tại hộp thoại tiếp theo, bạn nhấp chọn vào các mục sau:

- **Display password when audited:** Lựa chọn này cho phép hiển thị password khi chương trình đã crack xong.
- **Display how long it took to audit each password:** Hiển thị phương thức dò tìm những password dài.
- **Display audit method:** Hiển thị phương pháp tìm password.
- **Make visible notification when auditing is done:** Hiển thị thông báo khi quá trình dò tìm hoàn thiện.

5. Nhấp nút **Finish** để hoàn thành.

Password được tìm thấy và hiển thị trong giao diện của chương trình. Lưu ý, password được chương trình hiển thị ở hai dạng, chữ hoa và chữ thường. Mỗi tài khoản tương đương với một password (xem hình 2.20).

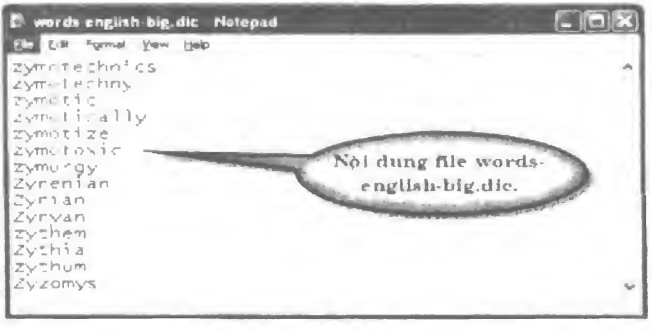


Hình 2.20: *Password được tìm thấy.*

2. Tìm lại password bằng từ điển

Để tìm password Windows bằng phương pháp này thì trước tiên bạn phải soạn thảo tập tin từ điển; hoặc sử dụng tập tin words-english-big.dic được chương trình cung cấp sẵn khi cài đặt.

Bạn có thể vào C:\Program Files\@stake\LC5 để mở file words-english-big.dic, sau đó thêm thông tin vào tập tin này (xem hình 2.21).



Hình 2.21: *Nội dung file words-english-big.dic.*

1. Sau khi thêm những thông tin cần thiết vào từ điển, bạn mở chương trình L0pCrack 5.02, vào **file > New Session** để mở giao diện làm việc mới.

2. Vào **File > LC5 Wizard**, màn hình LC5 Wizard xuất hiện, nhấp **Next** để tiếp tục.

3. Tiếp theo, nhấp chọn vào mục **Retrieve from the local machine** để tìm các tài khoản trong máy tính cục bộ, sau đó nhấp **Next** (xem hình 2.22).

Hình 2.22: *Tìm thông tin tài khoản từ máy tính cục bộ.*

4. Nhấp chọn mục **Custom**, tiếp theo nhấp nút **Custom Options**.

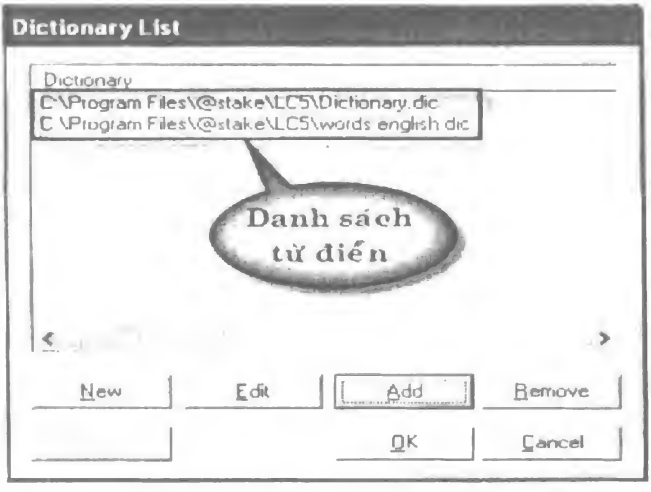
Mục này có chức năng cho phép tùy chỉnh danh sách từ điển và hash (xem hình 2.23).

Hình 2.23: *Những tùy chọn trong mục Custom.*

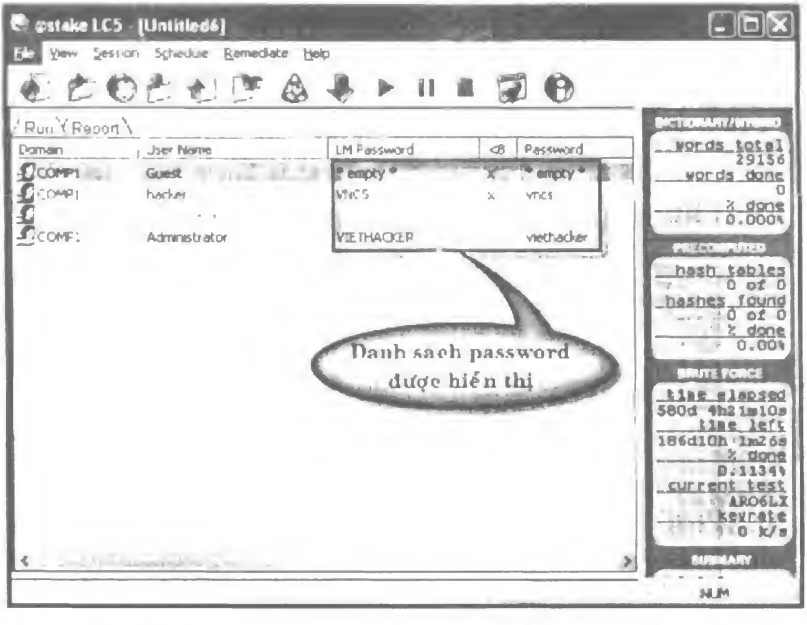
5. Nhấp nút **Dictionary List** để mở từ điển mà bạn vừa tạo. Tiếp theo nhấp nút **Add** để đưa từ điển vào danh sách, sau đó nhấp **OK** để áp dụng (xem hình 2.24).

6. Trong hộp thoại Custom Auditing Options, nhấp **OK** để áp dụng.

7. Tiếp theo bạn nhấp **Next** hai lần và nhấp **Finish** để thực hiện (xem hình 2.25).



Hình 2.24: *Thêm từ điển vào danh sách.*

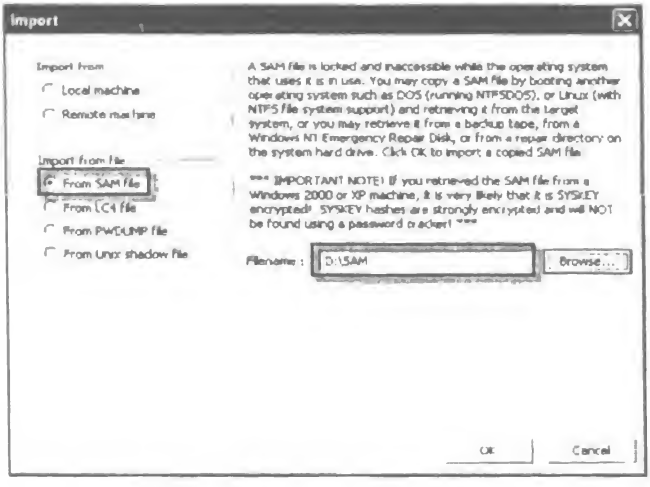


Hình 2.25: *Danh sách password được hiển thị.*

3. Tìm password Windows từ tập tin SAM

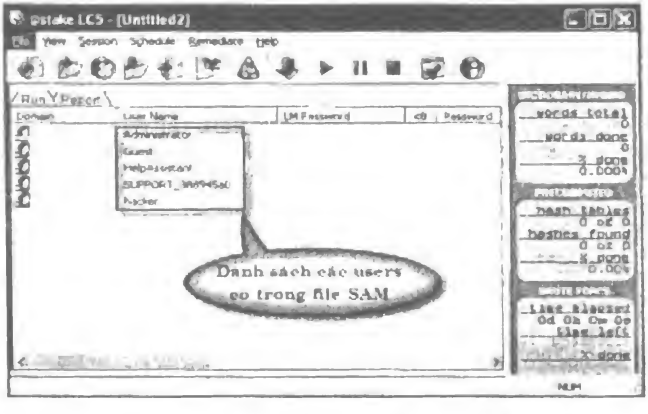
Bằng cách nào đó, bạn có được tập tin SAM của Windows để tìm thông tin trong tập tin này. Bạn có thể sử dụng LC5, các bước thực hiện như sau:

1. Tại giao diện chính của chương trình, vào menu **Session > Import**. Tiếp theo, nhấp chọn vào mục **From SAM file**.
2. Nhấp nút **Browse** để di chuyển đến thư mục chứa file SAM, ví dụ **D:\SAM**, sau đó nhấp **OK** (xem hình 2.26).



Hình 2.26: *Đưa file SAM vào.*

3. Sau khi Import file SAM vào chương trình, nội dung của file SAM được hiển thị trong giao diện chính của chương trình (xem hình 2.27).



Hình 2.27: *Nội dung file SAM.*

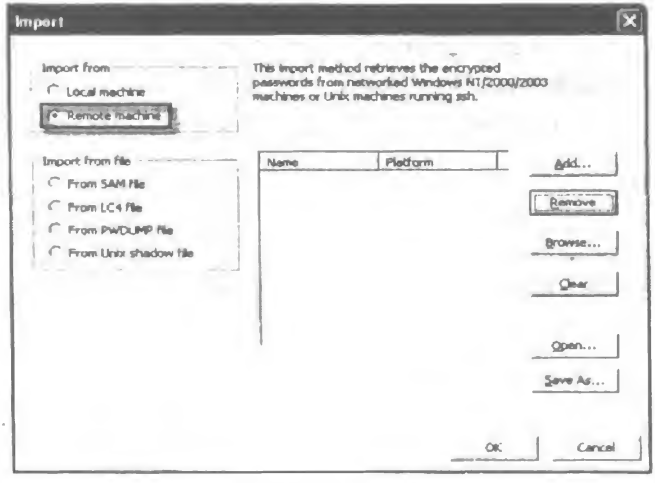
4. Tiếp theo, bạn tiến hành tìm password bằng phương pháp như đã trình bày trên.

4. Tìm lại password Windows Server 2003 qua LAN

Chương trình có tiện ích giúp bạn tìm lại password Windows qua mạng LAN. Để tìm được password bằng tiện ích này, yêu cầu bạn phải có đặc quyền quản trị trên hệ thống Windows Server. Cách thực hiện như sau:

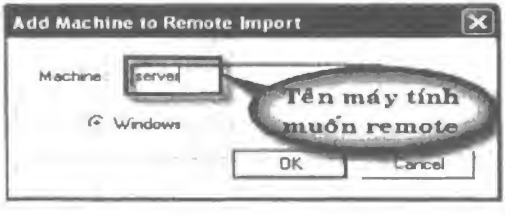
1. Tại giao diện chính của chương trình, vào menu **Session > Import**.
2. Nhấp chọn vào **Remote machine** (xem hình 2.28).

Mục này chỉ áp dụng cho hệ điều hành Windows NT/2000/2003 và Unix.



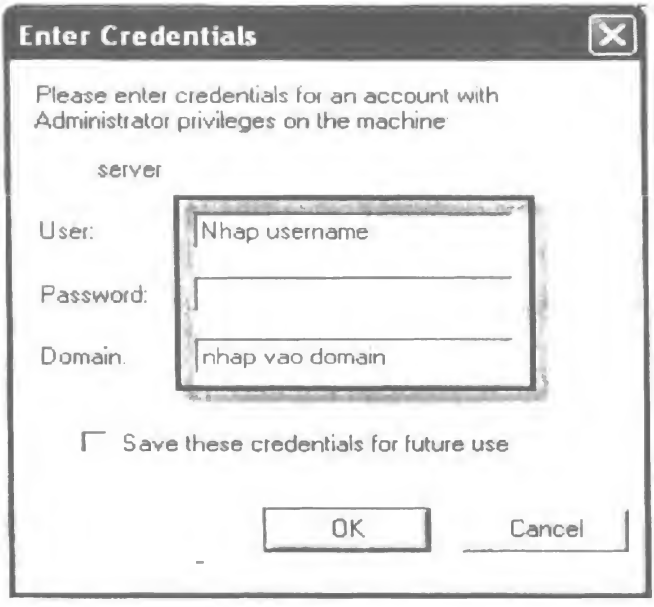
Hình 2.28: *Chọn Remote machine.*

3. Tiếp theo, nhấp nút **Add**, sau đó nhập vào tên máy tính muốn remote, ví dụ **server**, sau đó nhấp **OK** (xem hình 2.29).



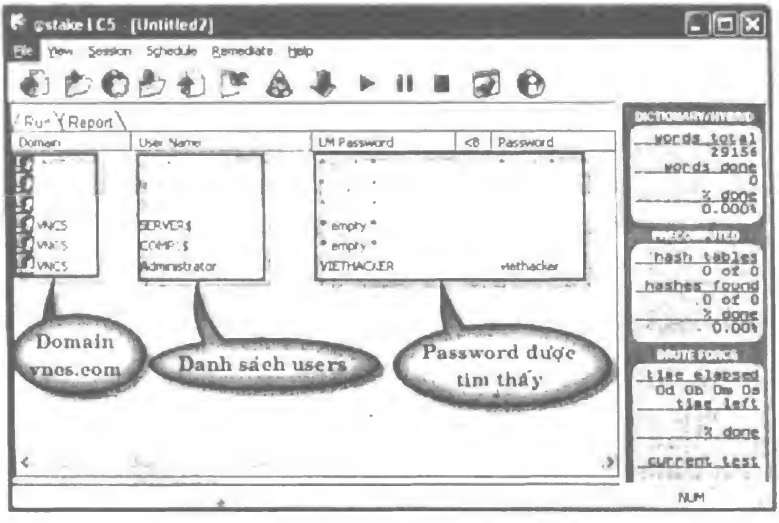
Hình 2.29: *Nhập vào tên máy tính muốn remote.*

4. Tiếp theo, nhập vào username, password và tên domain của máy tính muốn tìm password (xem hình 2.30).



Hình 2.30: *Nhập thông tin đăng user và domain.*

5. Sau khi danh sách các tài khoản được hiển thị trong giao diện chính của chương trình, bạn tiến hành dò tìm như cách đã giới thiệu ở trên (xem hình 2.31).



Hình 2.31: *Password được tìm thấy.*

Hướng dẫn thêm:

- Ngoài những chức năng chính như đã giới thiệu trong phần trên, chương trình còn cho phép bạn tìm password từ những tập tin

LC4 (đây là những files từ chương trình L0pCrack có phiên bản cũ hơn), PWDUMP, và các file shadown của hệ điều hành Unix và nhiều tính năng khác nữa. Bạn có thể tham khảo thêm khi sử dụng chương trình.

- **Brute-Force (thử sai):** Là phương pháp kiểm tra tất cả các trường hợp của chuỗi password có chiều dài nhỏ (chuỗi password có chiều dài nhỏ hơn 5 hoặc 8 ký tự). Ưu điểm của phương pháp này là nó có thể tìm ra password nhanh chóng. Tuy nhiên, không phải tất cả các trường hợp đều có thể tìm ra password, vì chuỗi password có độ dài lớn hơn 16 ký tự và tuân theo các quy tắc đặt password thì phương pháp Brute-Force không khả thi do thời gian tìm sẽ rất lâu. Để khắc phục hạn chế này, phương pháp dò tìm password bằng từ điển ra đời.
- **Tìm password bằng từ điển (dictionary):** Đây là phương pháp dò tìm password dựa vào tâm lý đặt password của người dùng như: Họ tên, ngày tháng năm sinh, một số sự kiện,... Các chương trình dò tìm password sẽ so sánh từng từ trong từ điển với chuỗi password của tài khoản người dùng để tìm. Tuy nhiên, không phải password nào cũng tìm thấy do ngôn ngữ ở mỗi Quốc gia khác nhau. Ví dụ, ở Việt Nam hay Trung Quốc những từ như: emyeu, bonghong, thanai thì phương pháp từ điển không khả thi.

V. Windows Password Cracker V. 2.1.9.0

Khi có được file SAM của hệ điều hành thì công việc tiếp theo là giải mã password có trong files này. Một trong những phần mềm hay nhất giúp giải mã files này là Windows Password Cracker. Chương trình cung cấp hai cách giải mã cơ bản đó là Brute-force (thử sai) và Dictionary (từ điển).

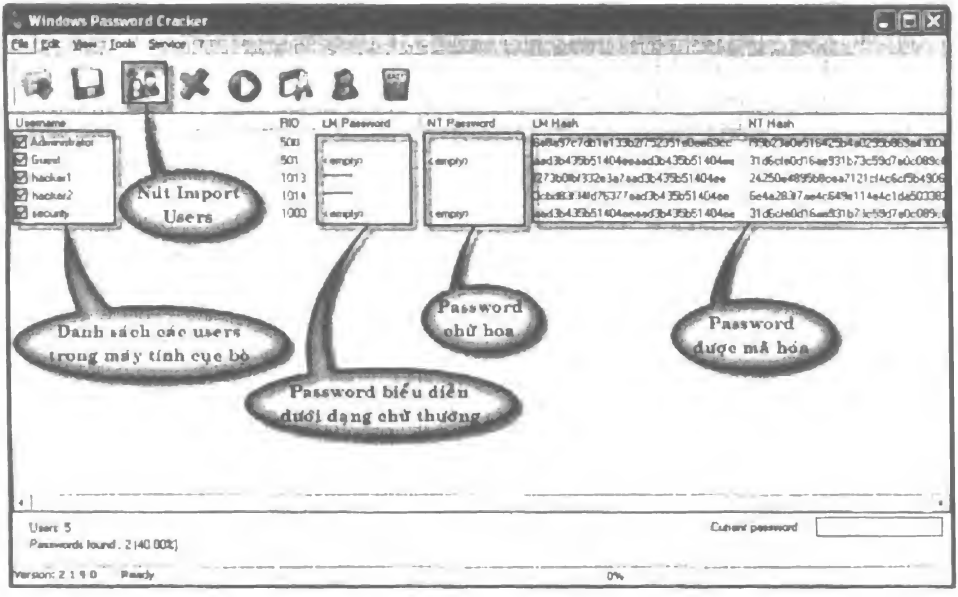
Bạn có thể download chương trình này tại website www.minhkhai.com.vn, thư mục Chapter 2. Sau khi giải nén và cài đặt, bạn thực hiện như sau:

1. Tìm lại password bằng phương pháp Brute-force

Sau khi cài đặt Windows Password Cracker, để tìm password của các users trong máy tính cục bộ bạn thực hiện như sau:

1. Vào **Start > Programs > Windows Password Cracker > Windows Password Cracker** để chạy chương trình. Giao diện như hình 2.32.

2. Nhấp nút **Import Users**, chương trình sẽ tự động nhập các users hiện có trong máy tính vào danh sách ở giao diện chính của chương trình (xem hình 2.32).



Hình 2.32: *Danh sách các users trong máy tính.*

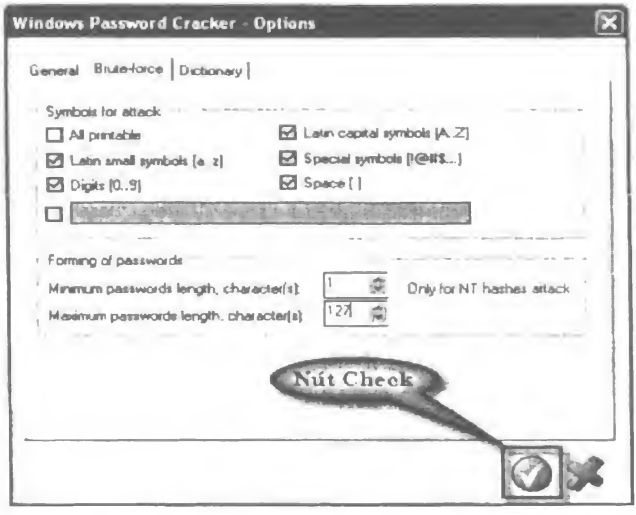
3. Vào menu **Service > Options** để mở hộp thoại **Windows Password Cracker – Options**, tiếp theo đánh dấu chọn vào các mục trong thẻ **General**:

- **Perform "intellectual" check of password:** Kiểm tra password bằng thuật toán thông minh.
- **Check early found password from twc.DIC:** Kiểm tra mật khẩu trong từ điển.

4. Nhấp chọn thẻ **Brute-force**, tiếp theo bạn đánh dấu chọn vào các mục sau:

- **Latin small simbols [a..z]:** Kiểm tra password bằng cách so sanh với các ký tự Latin thường từ a – z.
- **Digits [0..9]:** Các con số từ 0 – 9.
- **Latin capital simbols [A..Z]:** Các ký tự hoa từ A – Z.
- **Spectial Sombols [!@#$...]:** Các ký tự đặc biệt.
- **Space []:** Ký tự khoảng trắng.

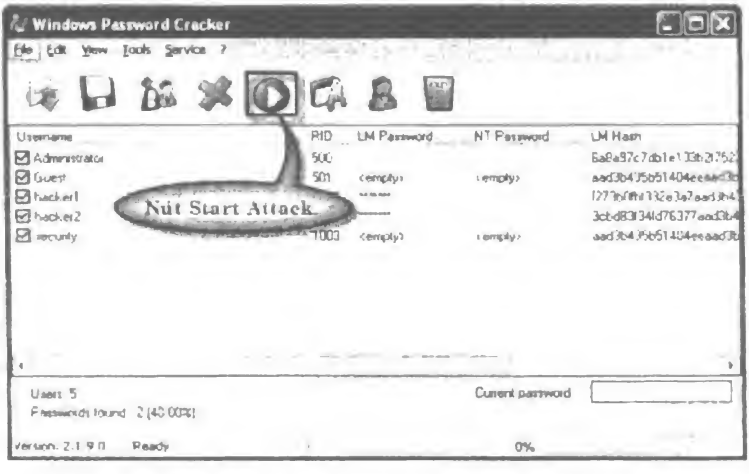
- **Minimum passwords length, character (s):** Độ dài nhỏ nhất của ký tự, bạn nhập là **1**.
- **Maximum passwords length, character (s):** Nhập vào độ dài lớn nhất của password. Mặc định là **127**, độ dài theo phân tích riêng của bạn. Sau đó, nhấp nút **Check** để áp dụng (xem hình 2.33).



Hình 2.33: *Crack password bằng Brute-force.*

5. Tiếp theo, nhấp nút **Start Attack** để tiến hành crack.

Ngoài ra, bạn có thể vào menu **Service > Start Attack** để thực hiện (xem hình 2.34).

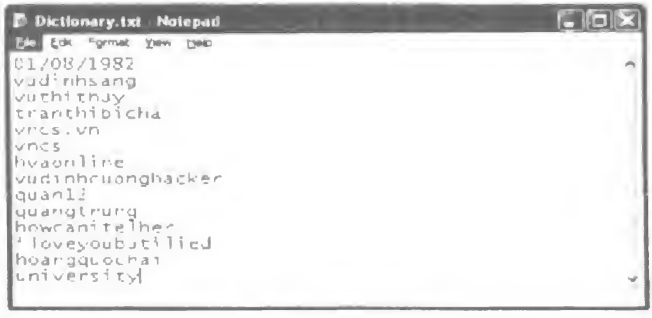


Hình 2.34: *Tiến hành Attack.*

2. Tìm Password bằng từ điển

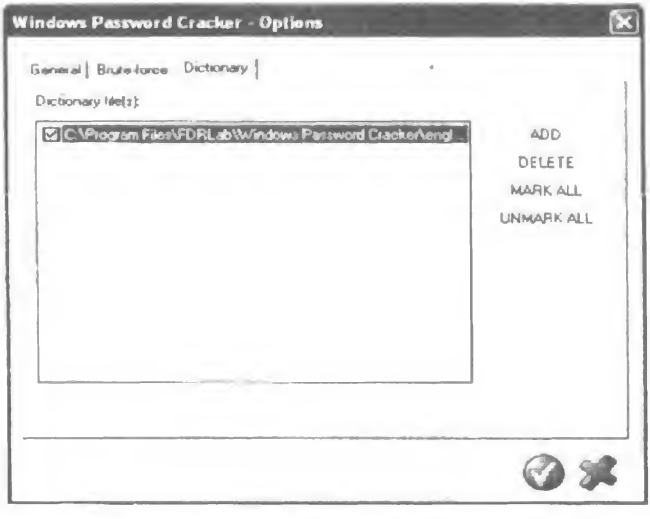
Để thực hiện tìm password bằng từ điển, trước tiên ta phải xây dựng một từ điển. Một từ điển hiệu quả thì nội dung của nó phải chứa những thông tin liên quan đến những người sử dụng máy tính mà chúng ta cần tìm password, ví dụ: Những thông tin liên quan đến ngày tháng năm sinh, sở thích, sở ghét, gia đình, bạn bè,...

Bạn mở nodepad và nhập các thông tin vào. Sau đó lưu chúng dưới dạng **dictionary.txt** hoặc **dictionary.dic**, hai định dạng này hay được các chương trình dò tìm password hỗ trợ (xem hình 2.35).



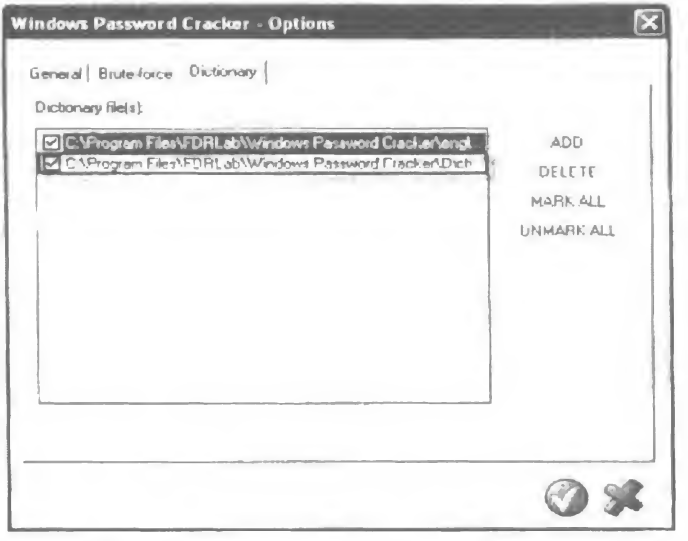
Hình 2.35: *Xây dựng từ điển.*

1. Thực hiện từ bước **1** đến bước **2** của mục "Tìm password bằng phương pháp Brute-force". Tiếp theo, trong hộp thoại Windows Password Cracker - Options chọn thẻ **Dictionary** (xem hình 2.36).



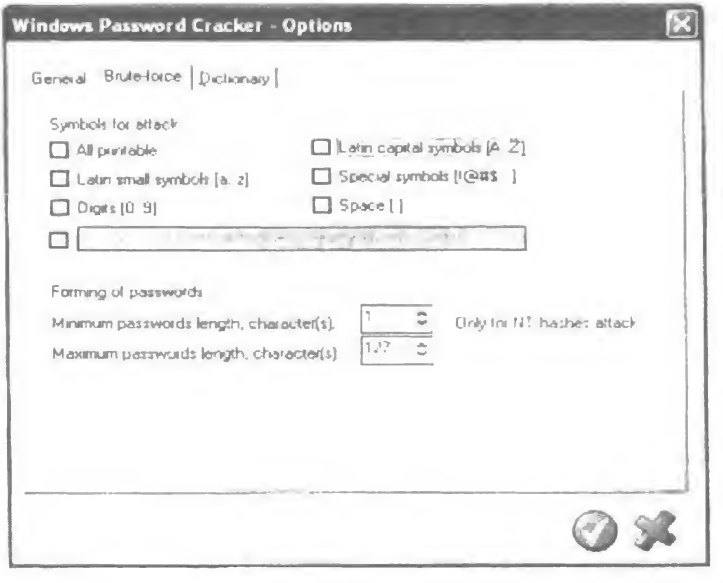
Hình 2.36: *Chọn thẻ Dictionary.*

2. Nhấp nút **Add** để đưa từ điển vào danh sách (xem hình 2.37).



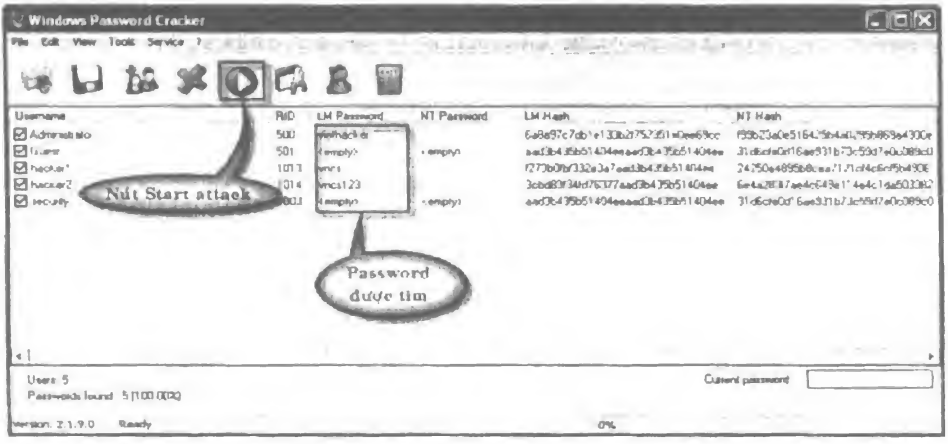
Hình 2.37: *Đưa từ điển vào danh sách.*

3. Tiếp theo, chọn thẻ **Brute-force**. Sau đó, bỏ chọn ở tất cả các mục trong thẻ này (xem hình 2.38).



Hình 2.38: *Bỏ chọn ở thẻ Brute-force.*

4. Nhấp nút **Check** để áp dụng, sau cùng nhấp nút **Start Attack** để tiến hành tìm (xem hình 2.39).

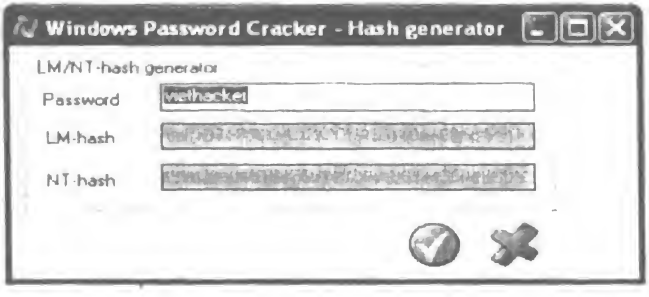


Hình 2.39: *Password được tìm thấy.*

3. Mã hóa dữ liệu

Để tiến hành mã hóa hoặc xem chuỗi ký tự được mã hóa ra sao, bạn vào menu **Tools > LM/NT - hash generator** để mở hộp thoại Windows Password Cracker Hash Generator.

Tại mục Password, nhập vào password để so sánh, ví dụ như **viethacker** (xem hình 2.40).



Hình 2.40: *Nhập password để so sánh.*

VI. Advanced Windows Password Recovery 2.9.2.224

Advanced Windows Password Recovery là chương trình để tìm tất cả các loại password Windows như: Password đăng nhập (để tìm được password này thì bạn phải có đặc quyền administrator), Password Screensaver, password .NET Passport, password RAS và dial-up, password của tài nguyên chia sẻ. Chương trình cũng hiển thị tất cả các users và groups, cho phép chạy bất kỳ một chương trình nào với tài

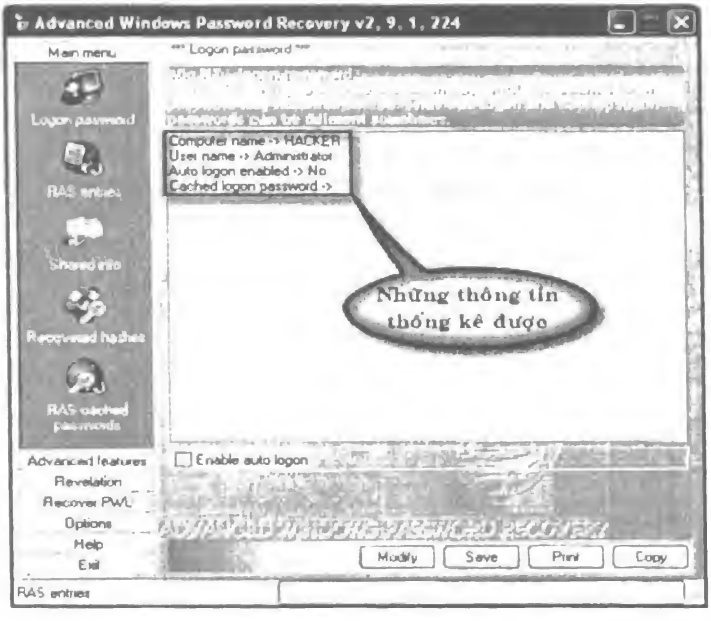
khoản khác, hiển thị password hashes, đọc password hashes từ files SAM và SYSTEM, hiển thị những password ẩn dưới các dấu sao (*). Bạn có thể tìm password theo hai hình thức Brute-force và Dictionary trong file PWL (đối với Windows 9x). Ngoài ra, nó còn hiển thị ID của Windows và Microsoft Office.

Sau khi giải nén và cài đặt chương trình, bạn thực hiện như sau:

1. Xác định password đăng nhập

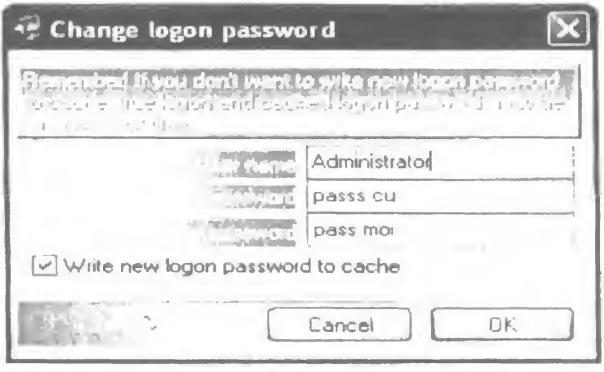
Chương trình này cho phép bạn xác định những thông tin liên quan đến quá trình đăng nhập như: Tên máy tính, tài khoản và chế độ tự động logon.

1. Để thực hiện, tại giao diện chính của chương trình, chọn mục **menu**, sau đó nhấp **Logon password**, đợi một lúc chương trình sẽ thống kê những thông tin liên quan đến quá trình đăng nhập và hiển thị trong ô bên phải (xem hình 2.41).



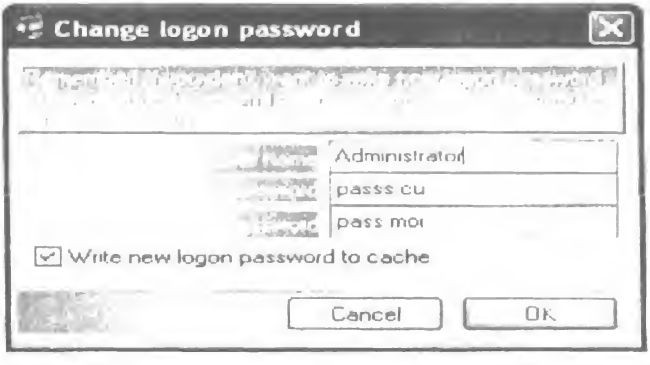
Hình 2.41: *Những thông tin thống kê.*

2. Tại mục Logon password nhấp nút **Modify**. Tiếp theo, nhập password cũ vào mục **Old password** và nhập password mới vào trong mục **New password** (xem hình 2.42).



Hình 2.42: *Đổi password cho tài khoản logon.*

3. Nếu chương trình kiểm tra quá trình đăng nhập vào máy tính với tài khoản đã chỉ định mà chưa đặt chế độ Auto logon thì mục chọn enable auto logon xuất hiện. Nếu muốn tự động đăng nhập với tài khoản administrator trong những lần đăng nhập sau thì nhấp chọn vào mục **Enable auto logon** để mở hộp thoại Confirmation. Tại hộp thoại này bạn nhập vào tài khoản cần logon tự động trong mục **Auto logon user name** và nhập vào password của tài khoản này trong mục **Auto logon password** (xem hình 2.43).



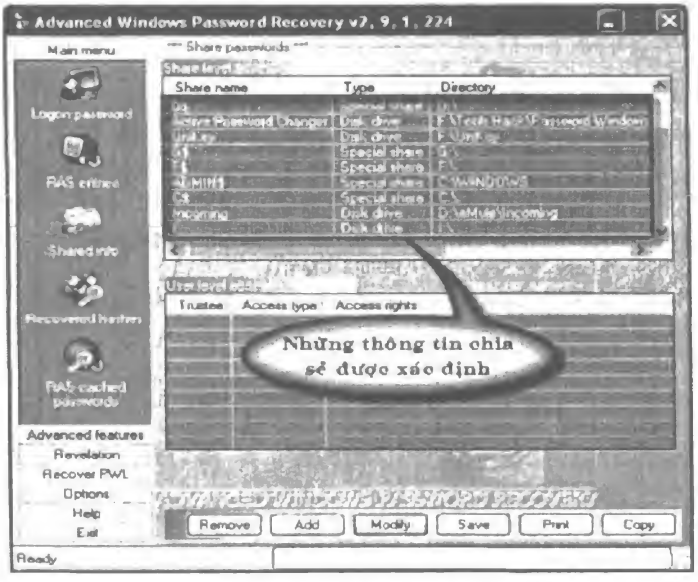
Hình 2.43: *Tự động logon.*

2. Xác định thông tin chia sẻ

Mục này cho phép bạn xác định những thông tin chia sẻ như các thư mục và ổ đĩa được chia sẻ trong máy tính cục bộ. Từ đó bạn có thể sửa những thông tin này, hoặc thêm những thư mục hoặc ổ đĩa chia sẻ. Các bước thực hiện như sau:

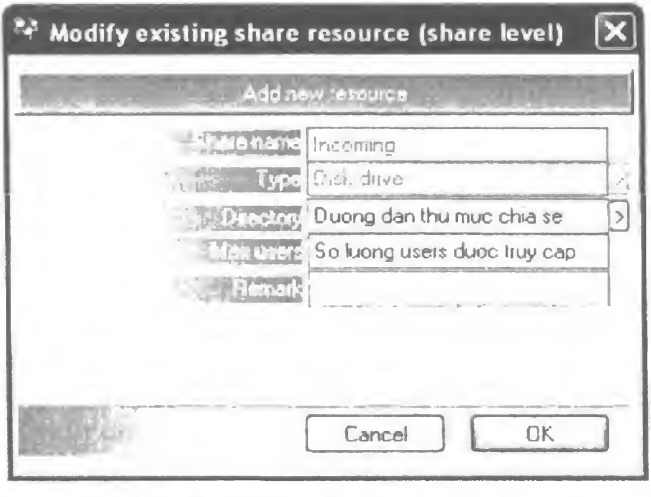
1. Trên giao diện chính của chương trình, chọn mục **menu**, tiếp theo nhấp chọn **Shared info**.

Chương trình sẽ hiển thị những thư mục và ổ đĩa được chia sẻ trong máy tính cục bộ (xem hình 2.44).



Hình 2.44: *Xác định những thông tin chia sẻ.*

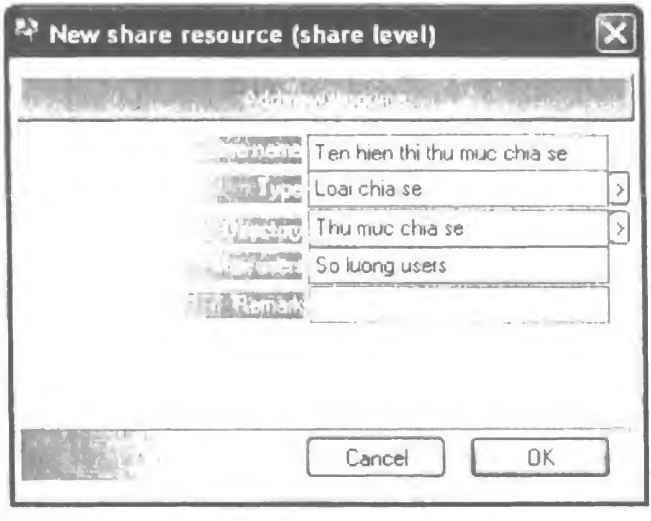
2. Nếu thấy những thông chia sẻ chưa hợp lý, bạn có thể chỉnh sửa lại bằng cách nhấp vào thư mục chia sẻ, sau đó nhấp nút **Modify** và nhập vào các thông tin như: Đường dẫn thư mục chia sẻ trong mục **Directory**, số lượng users được truy cập trong mục **Max Users** (xem hình 2.45).



Hình 2.45: *Chỉnh sửa thông tin chia sẻ.*

3. Bạn cũng có thể thêm những thư mục hoặc ổ đĩa chia sẻ. Để thực hiện, nhấp nút **Add**, sau đó nhập các thông tin chia sẻ như:

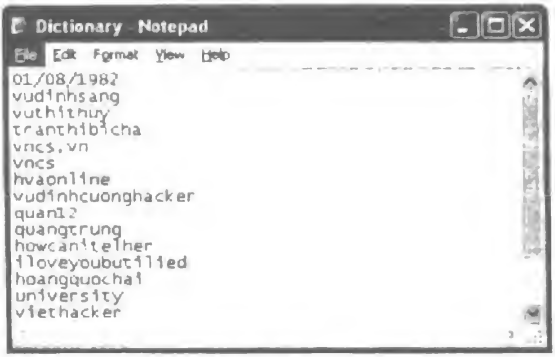
- **Share name:** Tên hiển thị của thư mục muốn chia sẻ.
- **Type:** Loại chia sẻ là một trong những loại được chỉ định sau.
- **Disk drive:** Ổ đĩa.
- **Print queue:** Hàng đợi máy in.
- **Communication device:** Thiết bị truyền thông.
- **Interprocess communication (IPC):** Chia sẻ theo IPC.
- **Special Share:** Chia sẻ đặc biệt.
- **Unknow:** Kiểu khác.
- **Directory:** Nhập vào thư mục chia sẻ của chương trình.
- **Max users:** Số lượng tối đa user được phép truy cập vào thư mục (xem hình 2.46).



Hình 2.46: *Chia sẻ thông tin.*

3. Tạo từ điển và Brute-force

Để tạo từ điển, bạn mở nodepad và nhập vào các thông tin liên quan đến các users trong máy tính, sau đó lưu lại với tên **Dictionary.dic** (xem hình 2.47).

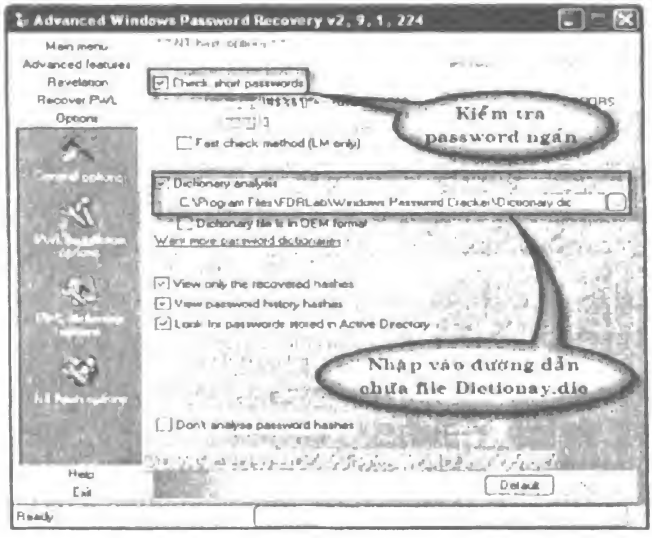


Hình 2.47: *Nội dung từ điển.*

1. Tại giao diện chính của chương trình, chọn mục **Options.** Tiếp theo, chọn mục **NT hash options**.

2. Đánh dấu chọn vào các mục sau:

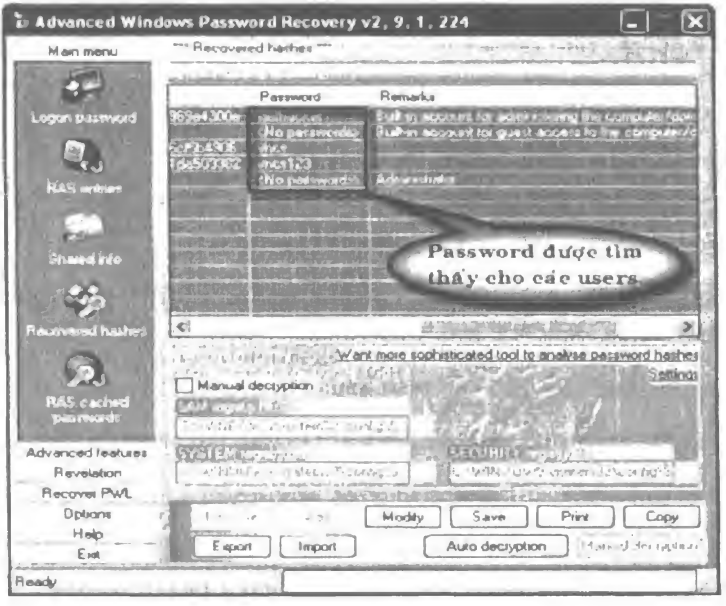
- **Check short password:** Kiểm tra các password ngắn.
- **Dictionary analysis:** Tại mục này nhập vào đường dẫn chứa file **Dictionary.dic** mà bạn vừa tạo.
- **View only the recovery hashes:** Xem password được tìm thấy.
- **View password History hashes:** Xem thông tin password.
- **Look for passwords stored in Active Directory:** Tìm password trong Active Directory (xem hình 2.48).



Hình 2.48: *Những thiết lập trong mục NT hash options.*

3. Nhấp chọn **Menu**, tiếp theo nhấp **Recovered hashes**.

Chương trình sẽ thực hiện tìm password của các users hiện có trong máy tính (xem hình 2.49).



Hình 2.49: *Password được tìm thấy.*

Hướng dẫn thêm:

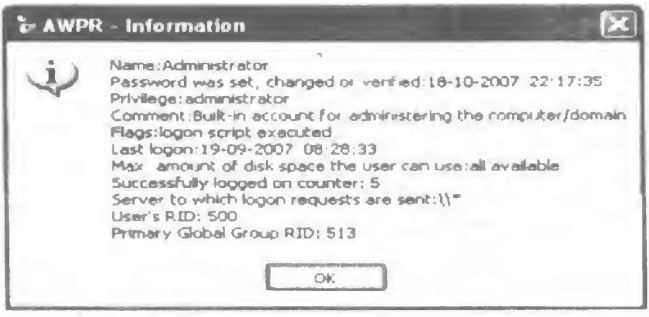
Mục này còn cho phép thay đổi hash của tài khoản được chọn. Để thực hiện, nhấp vào tài khoản muốn thay đổi, sau đó nhấp nút **Modify** và nhập vào hash tương ứng cho tài khoản.

4. Những chức năng nâng cao

Tại mục này chương trình cho ta những thông tin về tài khoản người dùng, thông tin về CD key của Windows và Office. Để thực hiện bạn làm theo các bước sau:

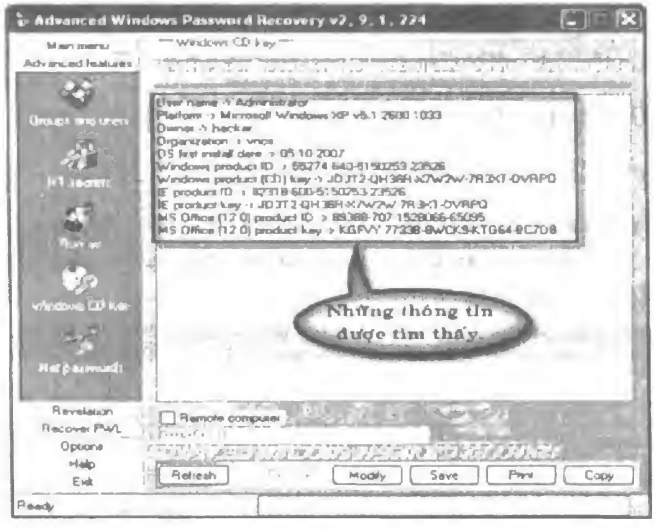
1. Tại giao diện chính của chương trình bạn chọn mục **Advanced features**.

2. Nhấp mục **Groups and Users**, chương trình thống kê những thông tin liên quan đến Group và Users. Để xem thông tin user administrator, nhấp phải chuột vào mục **Administrator > Administrator > View item info** (xem hình 2.50).



Hình 2.50: *Xem thông tin user administrator.*

3. Để xem những thông liên quan đến CD Key của Windows và Office, bạn nhấp vào mục **Windows CD Key** (xem hình 2.51).



Hình 2.51: *Những thông tin CD Key.*

VII. Proactive Windows Security Explorer™

Proactive Windows Security Explorer™ viết tắt PWSE[MT] là công cụ giúp kiểm tra độ an toàn của password trên Windows XP, NT, 2000. Đây là một công cụ hữu ích giúp cho quản trị viên xác định và triển khai hệ thống bảo mật password.

Chương trình hỗ trợ một số chức năng chính như: Kiểm toán, tìm lại password từ những files dump (pwdump/pwdump2/pwdump3), Registry của máy tính, registry ở dạng nhị phân (SAM/SYSTEM), bộ nhớ máy tính cục bộ và máy tính điều khiển từ xa, bao gồm cả Active Directory. Chương trình có thể sử dụng phương thức Brute-force hoặc Từ điển.

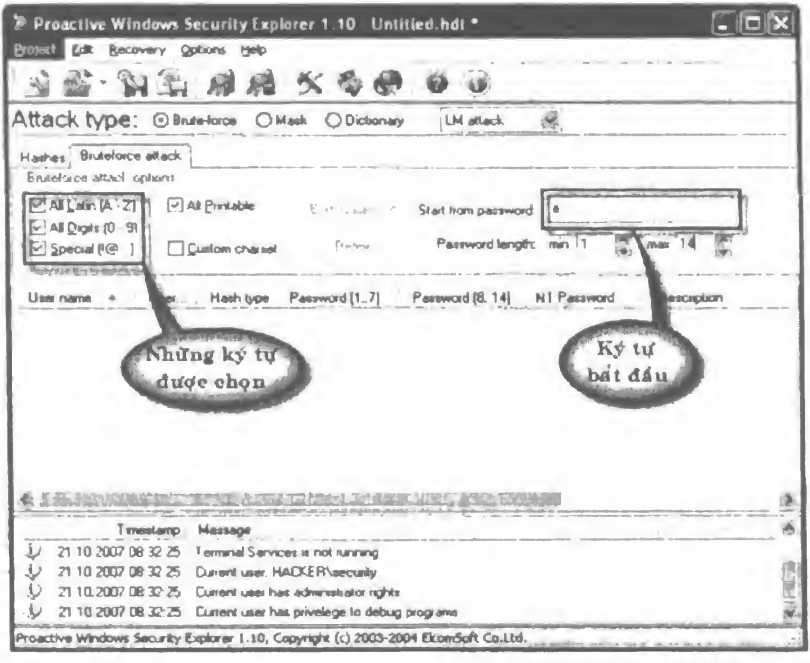
Sau khi giải nén và cài đặt chương trình vào máy tính, bạn thực hiện như sau:

1. Tài khoản và password trên máy tính cục bộ

Mục này cho phép bạn xác định tài khoản và kiểm tra password trên máy tính cục bộ, thực hiện như sau:

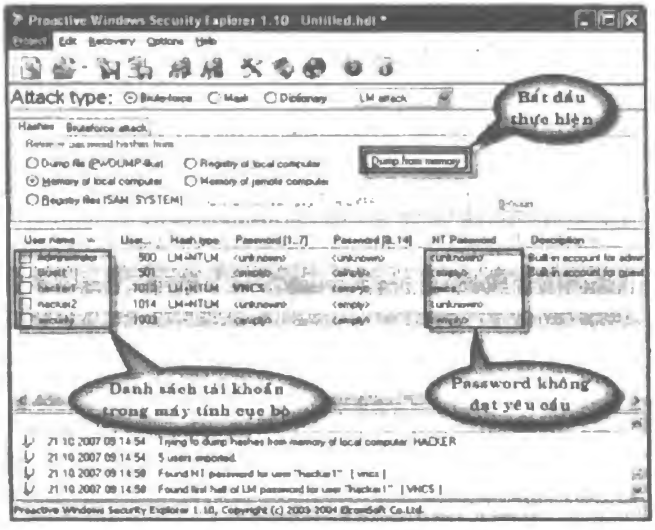
1. Vào **Start > Programs > Proactive Windows Security Explorer > Start > Programs > Proactive Windows Security Explorer** để mở chương trình.
2. Tại giao diện chính, nhấp vào mục **Brute-force**. Mục này cho phép bạn tìm lại password của tài khoản trong máy tính theo phương thức kết hợp các ký tự được chỉ định, thực hiện như sau:

- **All Latin [A - Z]:** Các ký tự Latin in từ A – Z.
- **All Digits [0 - 9]:** Tất cả các con số từ 0 – 9.
- **Special [!@...]:** Những ký tự đặc biệt.
- **Start from password:** Nhập ký tự đầu tiên để chương trình thực hiện. Với ký tự này chương trình sẽ thực hiện dò tìm từ ký tự bạn chỉ định (xem hình 2.52).



Hình 2.52: *Những thiết lập trong mục Brute-force.*

3. Chọn thẻ **Hashes**, sau đó nhấp chọn vào mục **Memory of local computer** để quét các tài khoản và password trong máy tính cục bộ. Sau cùng nhấp nút **Dump for memory** (xem hình 2.53).

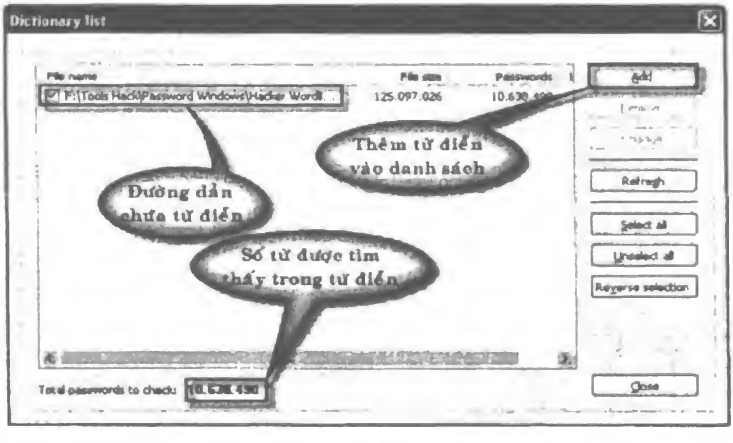


Hình 2.53: *Những thông tin được tìm thấy.*

2. Xác định password từ tập tin SAM và SYSTEM

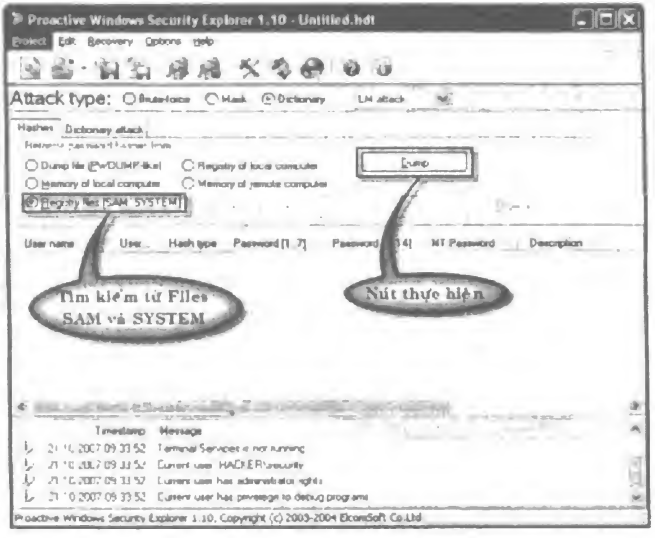
Để xác định thông tin các tập tin SAM và SYSTEM có trước, bạn có thể sử dụng tiện ích này. Ngoài ra, mục này còn cung cấp cho bạn một từ điển rất mạnh khoảng 10.638.490 từ. Để thực hiện, bạn làm như sau:

1. Nhấp chọn mục Dictionary, sau đó nhấp nút **Dictionary list**. Tiếp theo, nhấp **Add** để đưa từ điển vào danh sách (xem hình 2.54).



Hình 2.54: *Đưa từ điển vào danh sách.*

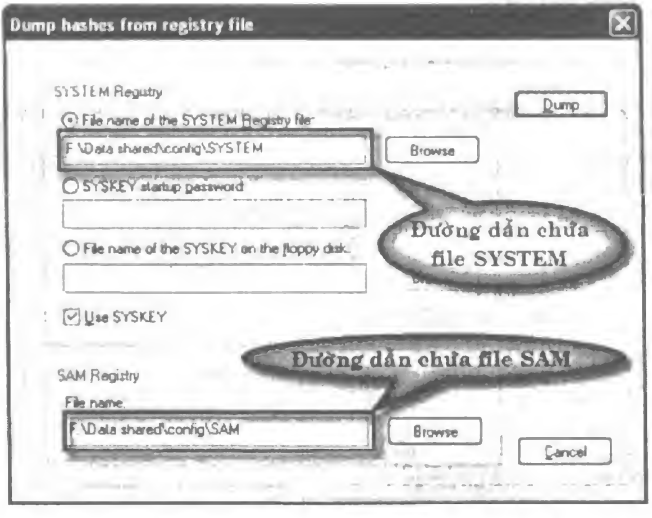
2. Nhấp chọn thẻ **Hashes** và nhấp chọn vào mục **Registry files (SAM, SYSTEM)**. Sau đó nhấp nút **Dump** để mở hộp thoại Dump hashes from registry file (xem hình 2.55).



Hình 2.55: *Tìm thông tin từ files SAM SYSTEM.*

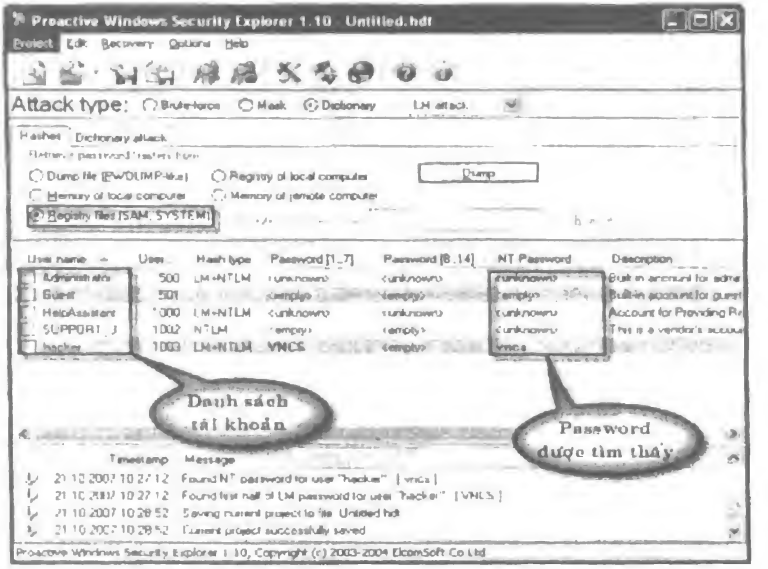
3. Nhấp chọn vào **File name of the SYSTEM Registry file**, tiếp theo nhấp **Browse** để đưa file SYSTEM vào.

4. Nhấp nút **Browse** ở mục SAM Registry để đưa file SAM vào. Sau cùng nhấp nút **Dump** để thực hiện (xem hình 2.56).



Hình 2.56: *Đưa File SAM và SYSTEM vào.*

5. Sau khi nhấp nút **Dump**, chương trình sẽ đưa danh sách các thông tin được hiển thị trên giao diện (xem hình 2.57).



Hình 2.57: *Những thông tin được tìm thấy.*

3. Xác định password qua LAN

Chương trình này còn cho phép bạn xác định độ an toàn password của bất kỳ một máy tính nào trong mạng. Chỉ cần ở một máy tính bất kỳ trong mạng LAN bạn cũng có thể kết nối đến một máy khác để tìm password và xác định độ an toàn của chúng. Phương pháp thực hiện như sau:

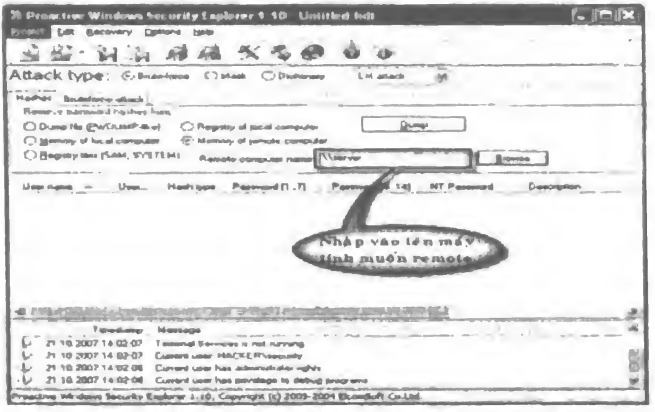
1. Tại giao diện chính, nhấp chọn thẻ **Hashes**, tiếp theo nhấp chọn **Memory of remote computer**.

2. Tại mục **Remote computer name**, bạn nhập tên máy tính muốn remote theo cú pháp:

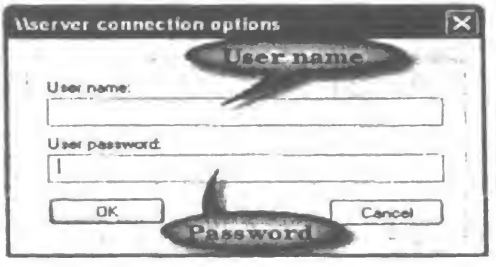
\\Tên máy tính muốn remote, ví dụ \\server, trong đó server là tên máy tính muốn remote, sau đó nhấp nút **Dump** để kết nối (xem hình 2.58).

Bạn cũng có thể nhấp nút **Browse** để hiển thị các máy tính đang chạy trong mạng LAN, sau đó chọn máy muốn kết nối.

3. Tiếp theo, bạn nhập username và password để chứng thực đăng nhập. Username phải là tài khoản administrator hoặc có đặc quyền tương đương với tài khoản này (xem hình 2.59).

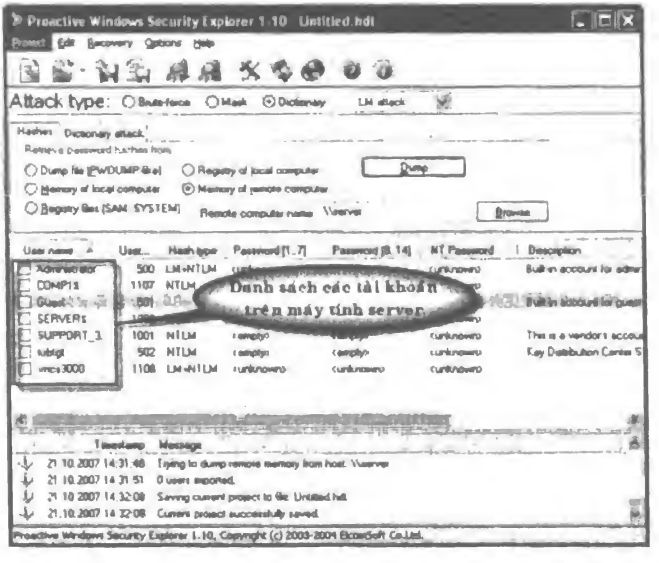


Hình 2.58: *Kết nối đến máy tính server.*



Hình 2.59: *Nhập username và password.*

4. Sau khi đăng nhập vào máy tính server, các thông tin mà chương trình tìm được hiển thị trong hình 2.60.



Hình 2.60: *Những thông tin thống kê được trên Server.*

VIII. Xem password đằng sau dấu sao (*)

1. See Password

Mỗi khi nhập password vào một mục nào đó, thay vì hiển thị password dưới những ký tự thông thường, chương trình hiển thị chúng dưới dạng những dấu sao (*) hay dấu chấm (•). Vậy làm thế nào để biết được những ký tự đằng sau những dấu * hay • này. Để giải quyết vấn đề này, bạn có thể sử dụng chương trình See Password.

Sau khi giải nén và cài đặt chương trình vào máy tính, bạn thực hiện như sau:

1. Vào **Start Programs > See Password > See password** để mở chương trình.
2. Nhấp vào bất kỳ vị trí nào trên giao diện của chương trình, đồng thời nhấn giữ chuột trái và kéo chương trình đến vị trí cần xem. Password được hiện ra đằng sau tấm gương của chương trình (xem hình 2.61).

Bạn áp dụng cách tương tự để xem password đằng sau dấu sao (*), hay dấu chấm (•) trên những chương trình khác nhau.

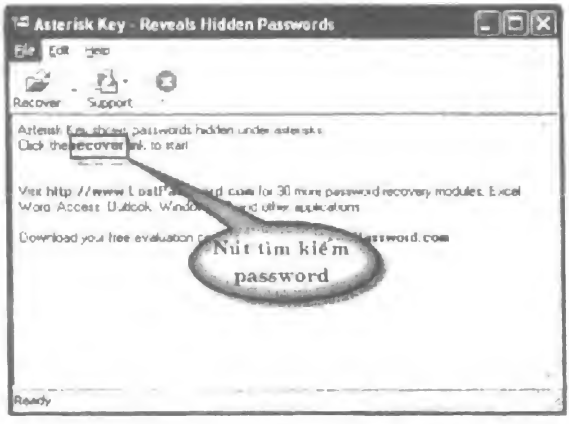
Hình 2.61: *Password được tim thấy bằng Seepass.*

2. Xem password bằng chương trình Asterisk Key

Asterisk Key không cần kéo và thả vào vùng cần xem password, hoạt động của chương trình tương đối dễ dàng. Khi bạn thấy một chương trình nào đó mà password của nó đang được hiện trong edit box (hộp soạn thảo) dưới dạng những dấu sao (*) hay dấu chấm (•) thì Asterisk Key là một giải pháp toàn diện giúp bạn hiển thị nhanh những password này.

Sau khi giải nén và cài đặt chương trình vào máy tính, bạn thực hiện theo các bước sau:

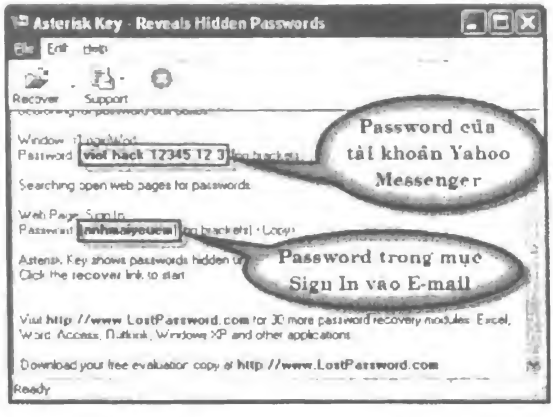
1. Vào **Start > Programs > Passware > Asterisk Key** để mở chương trình, giao diện chính của Asterisk Key như hình 2.62.



Hình 2.62: *Giao diện của Asterisk Key.*

2. Nhấp nút **Recovery** để tìm kiếm tất cả những password được hiển thị dưới dạng dấu sao (*) hoặc dấu chấm (•).

Lúc này, mọi password được che dấu bằng dấu sao (*) hoặc dấu chấm (•) đều được hiển thị (xem hình 2.63).



Hình 2.63: *Password được hiển thị.*

Hướng dẫn thêm:

Kỹ thuật xem password đằng sau dấu sao (*) chỉ có thể áp dụng trên một số hệ điều hành như: Windows XP (từ SP2 trở lại), Windows 2K. Đối với Windows XP SP3 hoặc Windows Vista thì kỹ thuật này không khả thi.

Chương 3:

TÌM LẠI PASSWORD TẬP TIN

- **Tìm lại password trên tập tin của Winrar.**
- **Tìm lại password trên tập tin của Winzip.**
- **Tìm lại password tập tin nén.**
- **Tìm lại password các tập tin của MS Office.**
- **Tìm password các tập tin của Adobe Acrobat Reader.**
- **Phương pháp đặt password cho các tập tin.**

Bạn đang thực hiện nghiên cứu một đề tài nào đó, và muốn tiếp cận với một số tài liệu chuyên ngành, chính vì vậy giải pháp đầu tiên là tìm thông tin trên Internet. Bạn đã mất nhiều thời gian và công sức để tìm kiếm và download tài liệu, nhưng một trong số chúng lại được bảo vệ bằng password, và không thể truy cập được.

Chương này sẽ giới thiệu đến bạn một số cách tìm lại password trên những tập tin của một số phần mềm thông dụng như MS Office, Winzip, Winrar và Adobe Acrobat.

Ngoài ra, chương này cũng giới thiệu đến bạn cách đặt password an toàn cho những loại tập tin trên.

I. Tìm lại password trên tập tin của Winrar

1. Chương trình Rar Password Recovery

Đây là một chương trình chuyên dụng, nó cho phép nhanh chóng tìm lại password trên những tập tin của Winrar.

Chương trình được cung cấp tại website www.minhkhai.com.vn, phần download. Sau khi giải nén và cài đặt, bạn thực hiện như sau:

1.1. Tìm password bằng phương pháp Brute-force

Phương pháp này rất hiệu quả để tìm lại những password có độ dài nhỏ. Để thực hiện, bạn làm như sau:

1. Vào **Start > Programs > Rar Password Recovery > Rar Password Recovery** để mở chương trình.
2. Nhấp nút **Open** để mở tập tin muốn tìm password.

Ví dụ tìm password tập tin có tên **Crack Tools.rar**.

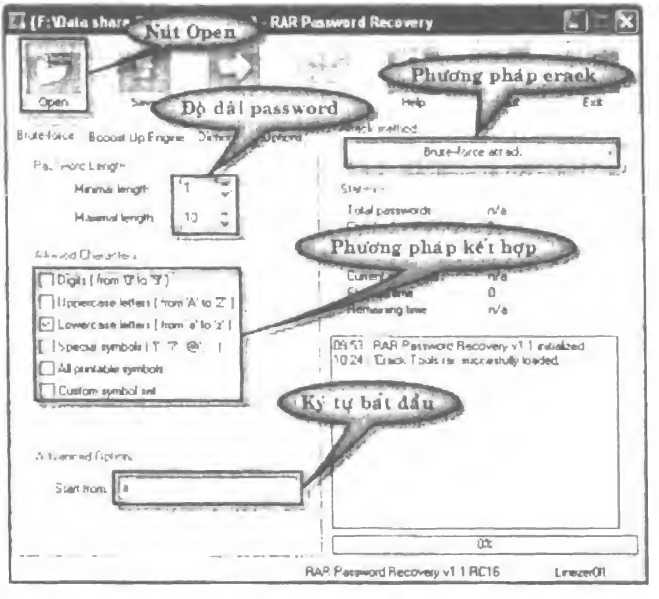
3. Tại mục Method attack, chọn **Brute-force attack**.
4. Tại thẻ Brute-force bạn chọn các mục thiết lập sau:

- **Digits (from '0' to '9'):** Các con số từ 0 đến 9.
- **Uppercase letters (from 'A' to 'Z'):** Ký tự hoa từ A–Z.
- **Lowercase letters (from 'a' to 'z'):** Ký tự thường từ a–z.
- **Special simbols** ('!', '?', '@'...): Các ký tự đặc biệt.
- **All printable simbols:** Tất cả các lựa chọn.

5. Tại mục **Start from**, nhập vào ký tự bắt đầu.

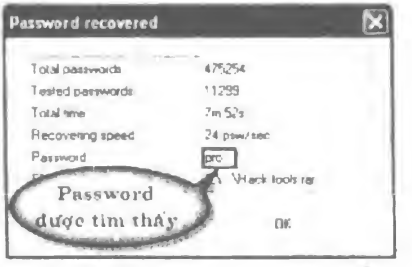
Căn cứ vào ký tự bạn nhập chương trình sẽ bắt đầu tìm và kết hợp ký tự này với những ký tự khác.

6. Tại mục Password length, ở **Minimal length**, nhập vào độ dài password nhỏ nhất; ở mục **Maximal length**, nhập vào độ dài lớn nhất của password (xem hình 3.1).



Hình 3.1: *Những thiết lập khi crack bằng Brute-force.*

7. Nhấp nút **Start**, chương trình tiến hành tìm kiếm, so sánh và giải mã. Sau cùng, nếu tìm thấy password chương trình sẽ xuất hiện hộp thoại thông báo như hình 3.2.



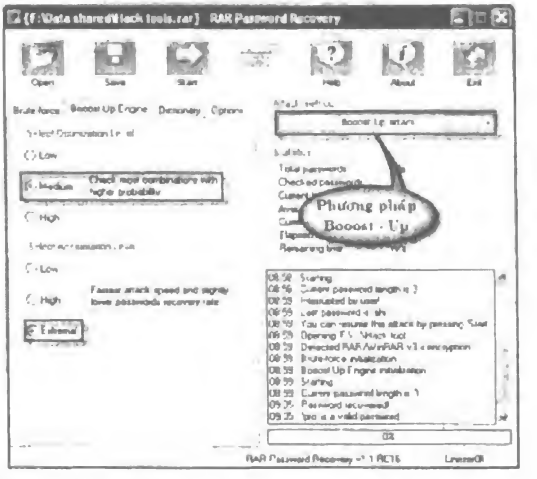
Hình 3.2: *Password được tìm thấy.*

1.2. Phương pháp Booost-Up Engine

Đây là phương cách đơn giản, những thiết lập trong thẻ này chỉ là những tùy chọn cho phép kết hợp những mục đã được định sẵn, sau đó chương trình sẽ tự xử lý. Để thực hiện bạn làm như sau:

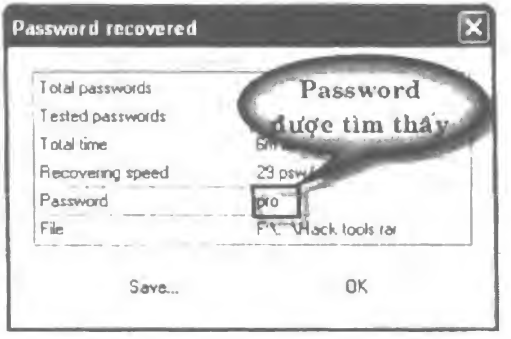
1. Nhấp nút **Open** để mở file .Rar mà bạn muốn tìm password.
2. Tiếp theo, trong mục Attack method, bạn chọn **Booost-Up.**
3. Chọn thẻ **Booost-Up Engine**, tiếp theo bạn nhấp chọn vào các mục sau:

- **Check most combinations with higher probability:** Mục này cho phép kết hợp những khả năng có thể xảy ra khi crack password.
- **Extremal:** Chọn mức kết hợp cao (xem hình 3.3).



Hình 3.3: *Phương pháp Booost-Up Engine.*

4. Sau khi quá trình xử lý kết thúc, chương trình sẽ cho chúng ta hộp thoại thông báo những thông tin tìm được như hình 3.4.

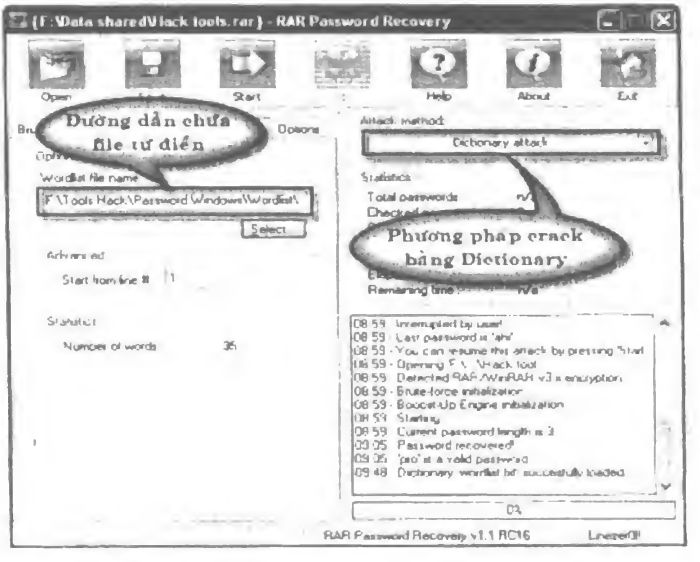


Hình 3.4: *Password được tìm thấy.*

1.3. Phương pháp từ điển

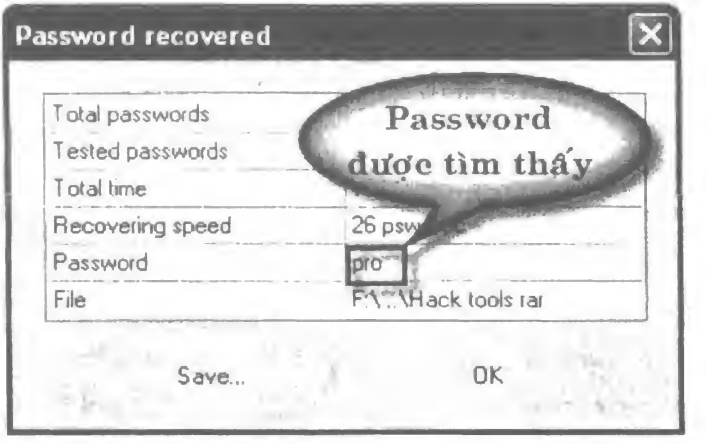
1. Nhấp nút **Open** để mở file .rar mà bạn muốn tìm password.
2. Trong mục Attack method, chọn **Dictionary**.
3. Chọn thẻ **Dictionary**, tiếp theo nhấp **Select** để mở tập tin từ điển đã tạo trước. Sau đó, nhập vào dòng đầu tiên trong từ điển, mặc định là 1 (để chương trình bắt đầu tìm từ vị trí dòng bạn nhập). Tiếp theo, nhấp nút **Start** để thực hiện.

Trong ví dụ này sử dụng tập tin **Wordlist.txt** (xem hình 3.5).



Hình 3.5: *Phương pháp crack password bằng từ điển.*

4. Sau khi quá trình xử lý hoàn thiện, chương trình sẽ thông báo đến bạn những thông tin mà nó tìm được (xem hình 3.6).



Hình 3.6: *Password được tìm thấy.*

2. Advanced Rar Password Recovery

Đây cũng là chương trình giúp tìm lại password cho những tập tin của Winrar.

Cách sử dụng tương tự như chương trình **Rar Password Recovery** trên.

II. Tìm lại password trên tập tin của Winzip

1. Advanced Zip Password Recovery

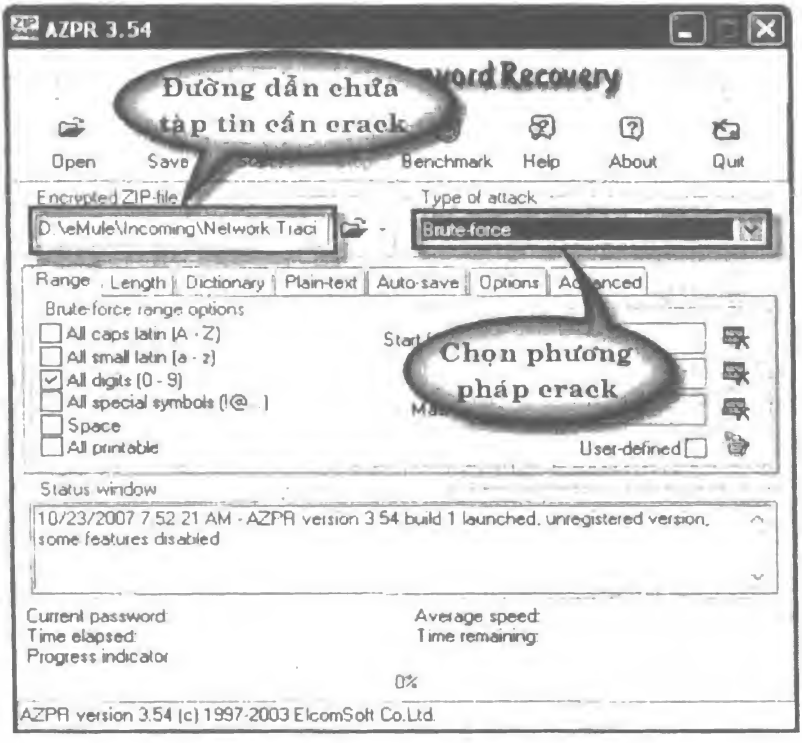
Những tập tin có định dạng .zip được sử dụng khá phổ biến, vì Winzip là một trình nén dữ liệu rất hay. Hơn nữa, Winrar ngoài định dạng .rar mặc định, chương trình còn hỗ trợ nén và giải nén dạng .zip. Chính vì vậy mà những tập tin .zip có rất nhiều trên Internet.

Sau khi giải nén và cài đặt chương trình, bạn thực hiện như sau:

1.1. Phương pháp Brute-force

1. Vào **Start > Programs > Advanced Zip Password Recovery > Advanced Zip Password Recovery** để mở chương trình.
2. Nhấp **Open** để mở tập tin .zip muốn tìm password. Ví dụ, tìm password tập tin **Winice.zip**.

3. Trong mục Type of attack, chọn **Brute-force**, để dò tìm bằng phương pháp kết hợp các ký tự (xem hình 3.7).

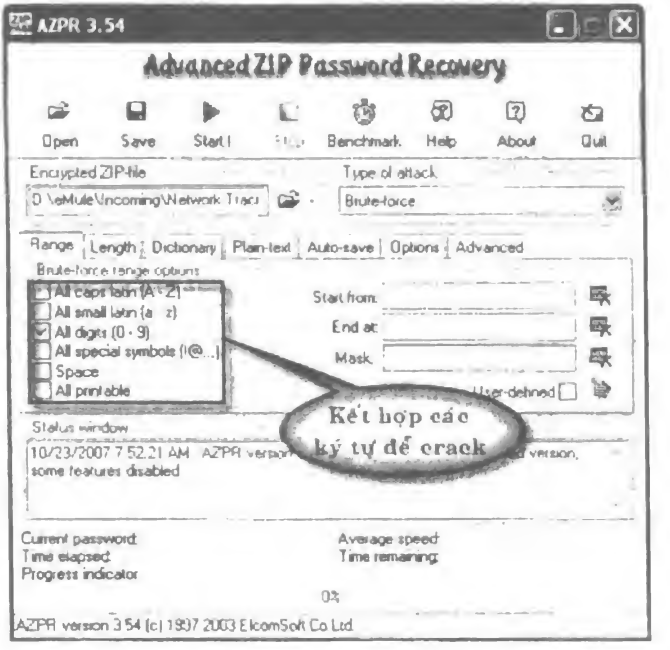


Hình 3.7: *Chọn tập tin và phương pháp crack.*

4. Tiếp theo, nhấp chọn thẻ **Range** và tham khảo các mục sau:

- **All caps latin [A-Z]:** Tất cả các ký tự Latin hoa từ A – Z.
- **All small latin [a-z]:** Các ký tự Latin thường từ z – z.
- **All digits:** Tất cả các ký tự số từ 0 – 9.
- **All special simbols [!@...]:** Tất cả các ký tự đặc biệt.
- **Space:** Ký tự khoảng trắng.
- **All printable:** Kết hợp tất cả các từ (xem hình 3.8).

5. Chọn thẻ **Length**, sau đó nhập độ dài nhỏ nhất trong mục **Minimum password length**, mặc định là 1 và độ dài lớn nhất của password trong mục **Maximum password length** là 100.

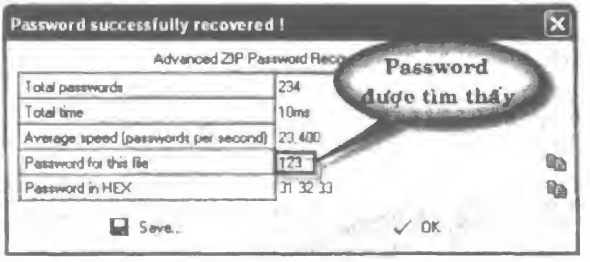


Hình 3.8: *Kết hợp các ký tự để crack.*

Nên thiết lập password có độ dài vừa phải, nếu để dài quá thì tìm password sẽ mất rất nhiều thời gian (xem hình 3.9).

Hình 3.9: *Những thiết lập trong thẻ Length.*

6. Nhấp nút **Start** để thực hiện. Sau khi quá trình tìm kiếm hoàn thiện, chương trình sẽ xuất ra một bảng thông báo cùng với password mà chương trình đã tìm thấy (xem hình 3.10).



Hình 3.10: *Password được tìm thấy.*

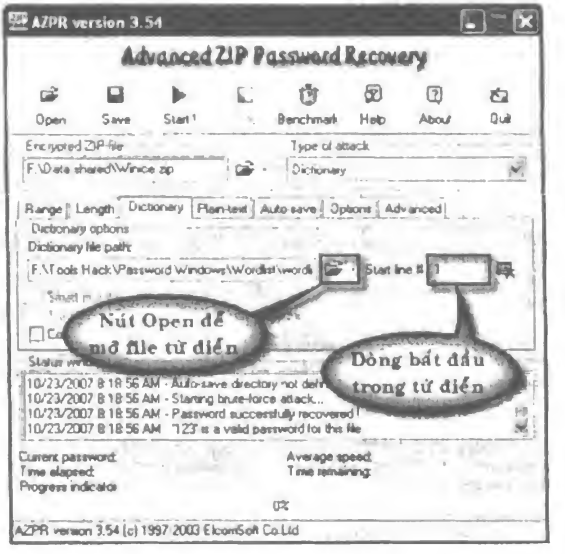
1.2. Phương pháp tìm password bằng từ điển

1. Nhấp nút **Open** để mở tập tin .zip muốn tìm lại password.
2. Tiếp theo, trong mục Type of attack, bạn chọn **Dictionary**.

Mục này cho phép bạn chọn phương pháp dò tìm.

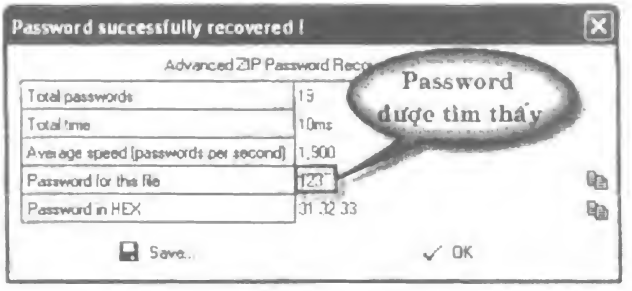
3. Nhấp nút **Open** để mở tập tin mà bạn muốn làm từ điển. Sau đó, bạn nhập vào dòng đầu tiên để chương trình tham chiếu trong từ điển ở mục **Start line**.

Loại từ điển phải có định dạng .dic, ví dụ, sử dụng từ điển **Wordlist.dic** để tìm password tập tin **Winice.zip** (xem hình 3.11).



Hình 3.11: *Những thiết lập trong thẻ Dictionary.*

4. Nhấp nút **Start** để thực hiện. Sau khi hoàn thành, chương trình sẽ cho chúng ta bảng thông báo với password được tìm thấy (3.12).



Hình 3.12: *Password được tìm thấy.*

III. Tìm lại password tập tin nén

1. Advanced Archive Password Recovery 3.01

Đây là chương trình cho phép tìm password trên các loại tập tin như:

- ZIP/PKZip/WinZip.
- ARJ/WinARJ.
- ACE/WinACE (1.x).
- RAR/WinRAR.

Chương trình hỗ trợ rất nhiều dạng tập tin như đã trình bày. Với máy tính có cấu hình Pentium IV như ngày nay thì việc tìm password sẽ thực hiện rất nhanh, phương pháp thực hiện và so sánh khoảng 15 triệu password trong trên một giây. Ngoài việc tìm password bằng phương pháp Brute-force truyền thống, chương trình này còn cho phép crack bằng Dictionary.

Sau khi giải nén và cài đặt chương trình, bạn thực hiện như những mục trước để tìm password.

2. Ultimate ZIP Cracker

Chương trình này cho phép bạn tìm lại password một số loại tập tin của những chương trình như: Winzip, MS Word, Excel, và những tập tin thực thi như .exe.

Nó có thể làm việc trên mọi loại phiên bản của các chương trình, ví dụ như nó có thể tìm password của MS Word 97/2000/2003. Password của các chương trình được tìm ra một cách nhanh chóng.

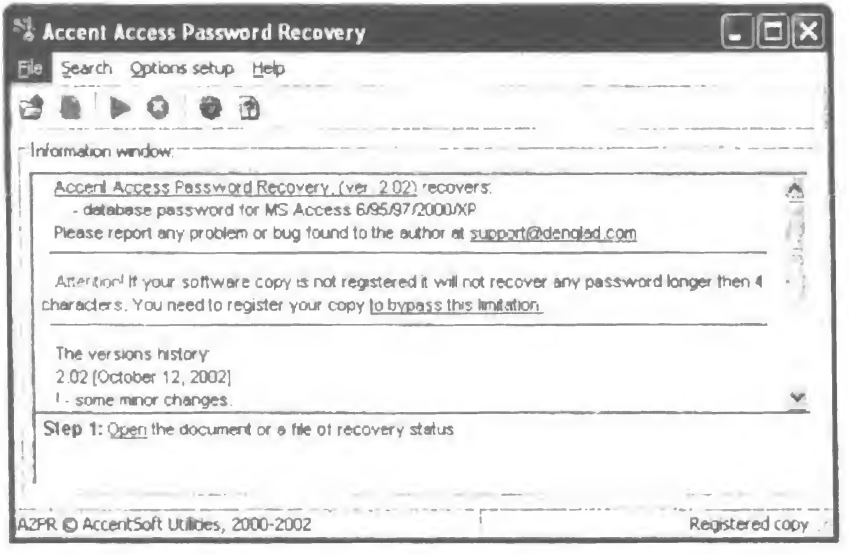
IV. Tìm password các tập tin của MS Office

1. Accent Access Password Recovery

Chương trình này cho phép tìm lại password trên những tập tin của MS Access (.mdb).

Sau khi giải nén và cài đặt chương trình, bạn có thể thực hiện theo các bước sau:

1. Vào **Start > Programs > Accent Access Password Recovery > Accent Access Password Recovery** để mở chương trình. Giao diện của chương trình như hình 3.13.



Hình 3.13: *Giao diện của Access Password Recovery.*

2. Nhấp nút **Open** để mở file có định dạng .mdb.

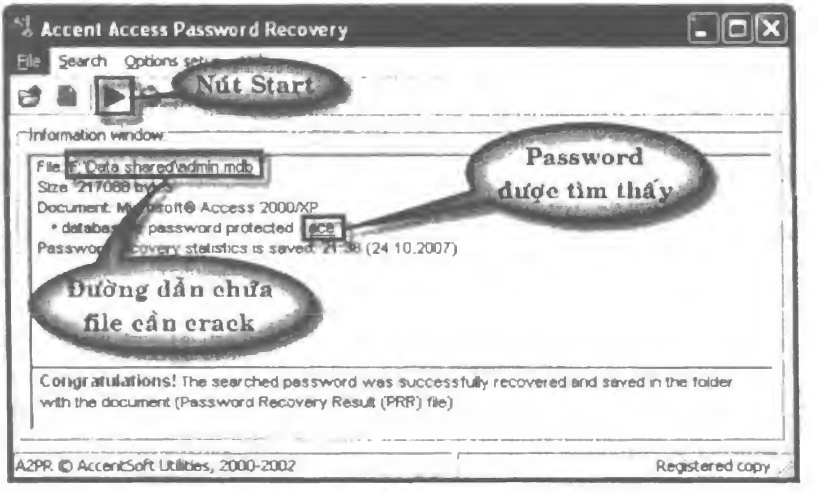
Ví dụ, tìm password của tập tin admin.mdb trong thư mục F:\Data shared\admin.mdb.

3. Nhấp nút **Start** để thực hiện.

Sau khi quá trình xử lý thành công, chương trình sẽ cho chúng ta password của file như hình 3.14.

Hướng dẫn thêm:

Chương trình này chỉ áp dụng để tìm những password có độ dài nhỏ. Nếu gặp những password có độ phức tạp cao thì ta không thể sử dụng chương trình này để tìm được, vì chương trình không cho phép áp dụng nhiều thiết lập phức tạp.



Hình 3.14: *Password được tìm thấy.*

2. Accent Office Password Recovery

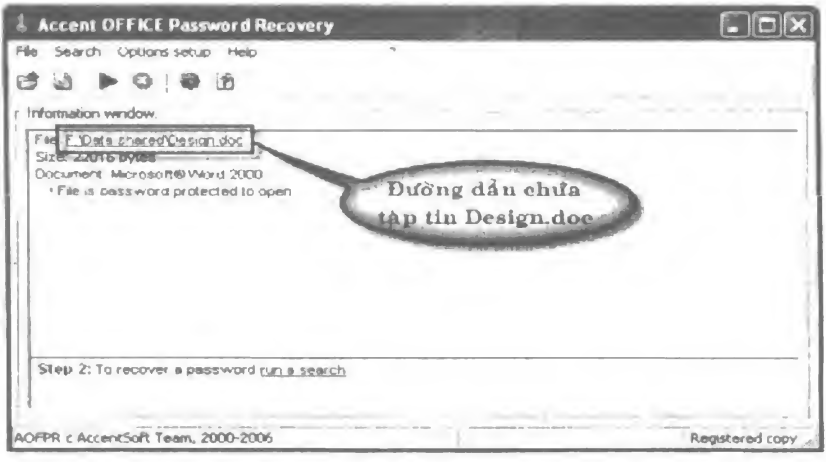
Đây là chương trình không chỉ có giao diện rất dễ sử dụng mà chức năng của nó cũng rất đa dạng, nó hỗ trợ bạn tìm password của nhiều loại tập tin như: MS Word, Excel, Access.

Sau khi giải nén và cài đặt chương trình, bạn thực hiện theo các bước sau.

2.1. Tìm password tập tin MS Word bằng phương pháp Brute-force

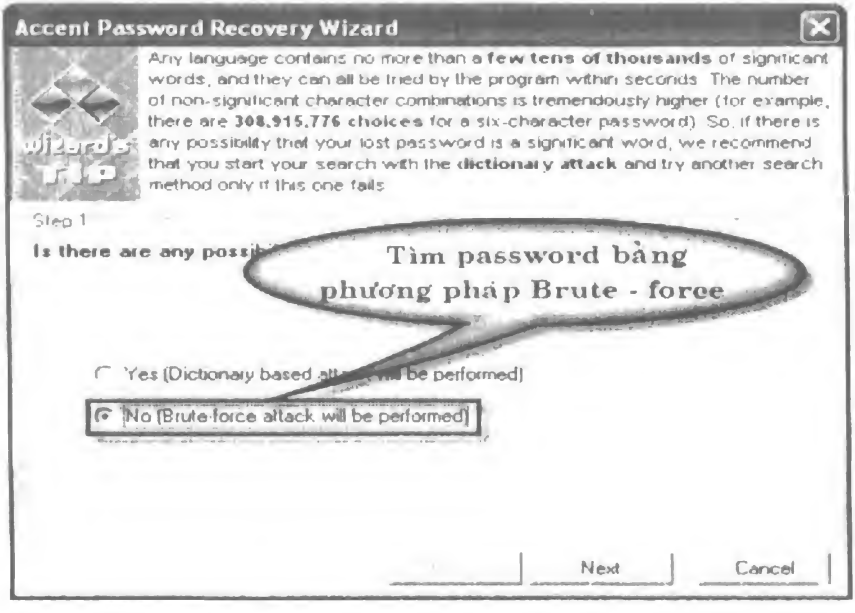
Giả sử ta có tập tin Design.doc được lưu trong thư mục F:\Data shared\Design.doc, chúng ta hãy sử dụng phương pháp Brute-force để tìm. Các bước thực hiện như sau:

1. Vào **Start > Programs > Accent Office Password Recovery > Accent Office Password Recovery** để mở chương trình.
2. Nhấp nút **Open** để mở tập tin Design.doc trong thư mục **F:\Data shared\Design.doc** (xem hình 3.15).



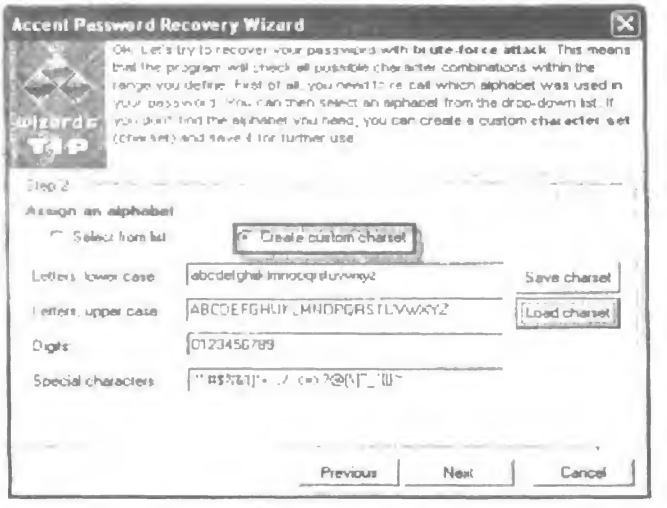
Hình 3.15: *Mở tập tin Design.doc.*

3. Tại giao diện chính của chương trình, vào menu **Search > Start Wizard** để mở hộp thoại Accent Password Recovery Wizard, nhấp chọn vào mục **No (Brute-force attack will be performed)**. Sau đó nhấp **Next** để tiếp tục (xem hình 3.16).



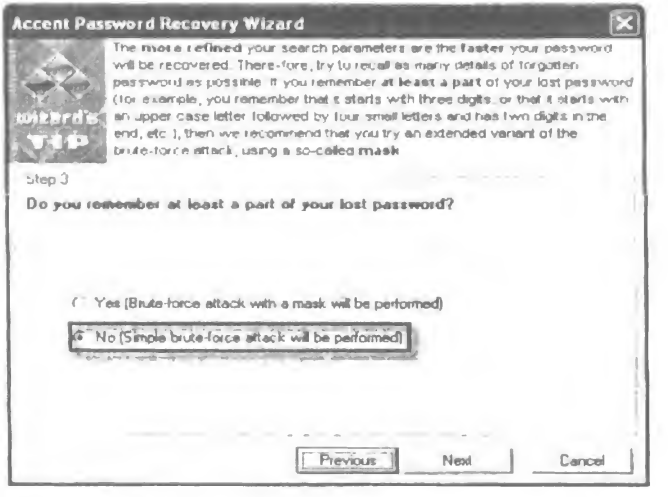
Hình 3.16: *Chọn phương pháp Brute-force.*

4. Tiếp theo, bạn nhấp chọn vào mục **Create custom charset**. Sau đó nhập vào chuỗi ký tự để chương trình thực hiện (xem hình 3.17).



Hình 3.17: *Nhập vào chuỗi ký tự để crack.*

5. Bạn nhấp chọn vào mục **No (Simple Brute-force attack will be performed)**. Sau đó nhấp **Next** để tiếp tục (xem hình 3.18).



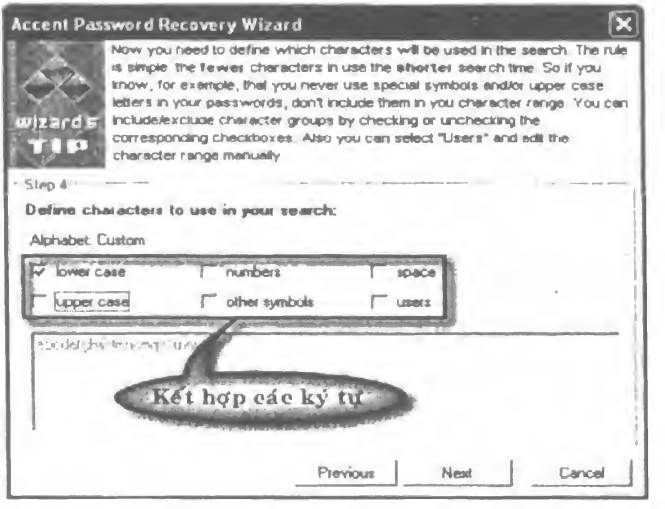
Hình 3.18: *Thực hiện crack bằng Brute-force.*

6. Tiếp theo bạn tham khảo các mục sau:

- **Lower case:** Các ký tự thường.
- **Upper case:** Các ký tự hoa.
- **Number:** Các ký tự số.
- **Other simbols:** Các ký tự đặc biệt.

- **Space:** Ký tự khoảng trắng.
- **Users:** Các ký tự do người dùng định nghĩa.

Tiếp theo, nhấp **Next** để tiếp tục (xem hình 3.19).

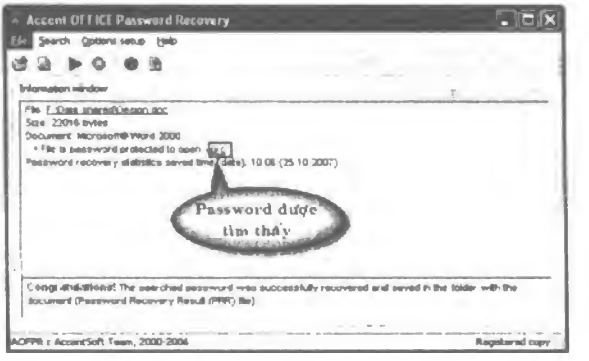


Hình 3.19: *Kết hợp các kiểu ký tự.*

7. Nhập vào độ dài nhỏ nhất của password trong mục **Password length from**, mặc định là **1**. Sau đó nhập ký tự bắt đầu trong mục **Start search with**, mặc định là **a**. Tiếp theo nhấp **Next** để tiếp tục (xem hình 3.20).

Hình 3.20: *Chọn độ dài và ký tự bắt đầu.*

8. Cuối cùng, bạn nhấp nút **Run search** để thực hiện. Sau khi xử lý xong, chương trình sẽ thông báo kết quả của việc tìm kiếm (xem hình 3.21).



Hình 3.21: *Password được tìm thấy.*

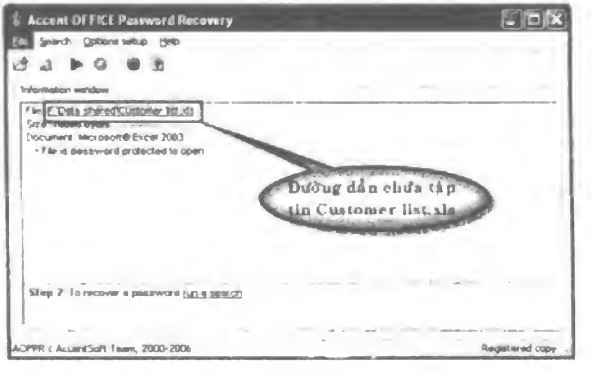
2.2. Tìm password tập tin của MS Excel bằng phương pháp từ điển

Trong mục này ta sẽ sử dụng kiểu từ điển để tìm password tập tin có định dạng .xls. Ví dụ, tìm password tập tin **Customer list.xls** trong thư mục F:\Data shared\Customer list.xls.

Để thực hiện được bước này, ta phải tạo ra một từ điển. Sau đó lưu nó dưới dạng .dic hoặc .txt. Các bước tạo từ điển như đã nói rõ trong chương 2.

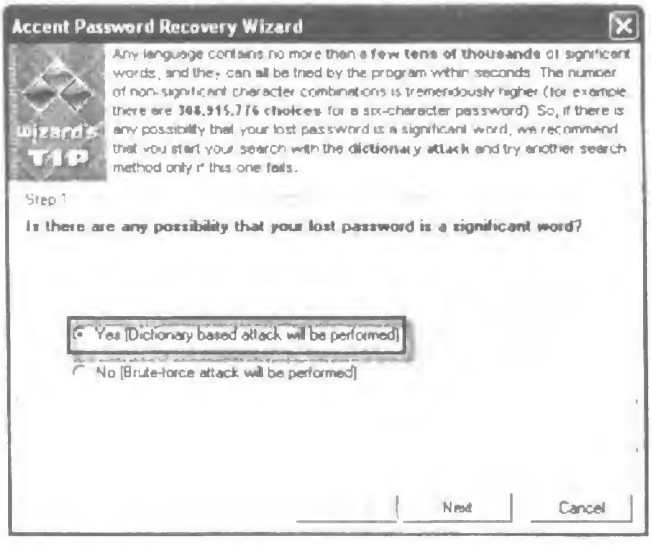
Ví dụ, sử dụng từ điển có tên Wordlist.txt, từ điển này bạn có thể download tại website www.minhkhai.com.vn.

1. Nhấp nút **Open** để mở tập tin **Customer list.xls** tại thư mục **F:\Data shared\Customer list.xls** (xem hình 3.22).



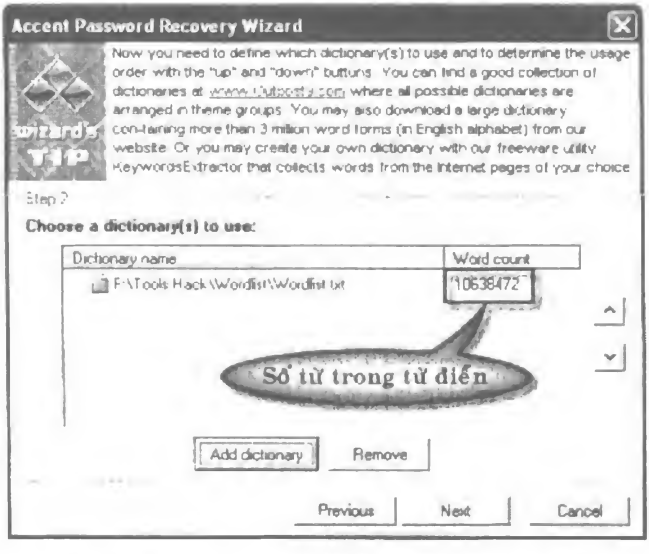
Hình 3.22: *Mở tập tin Customer list.xls.*

2. Tại giao diện chính của chương trình, vào menu **Search > Start Wizard** để mở hộp thoại Accent Password Recovery Wizard. Sau đó, chọn **Yes (Dictionary bases attack will be performed)** và nhấp **Next** để tiếp tục (xem hình 3.23).



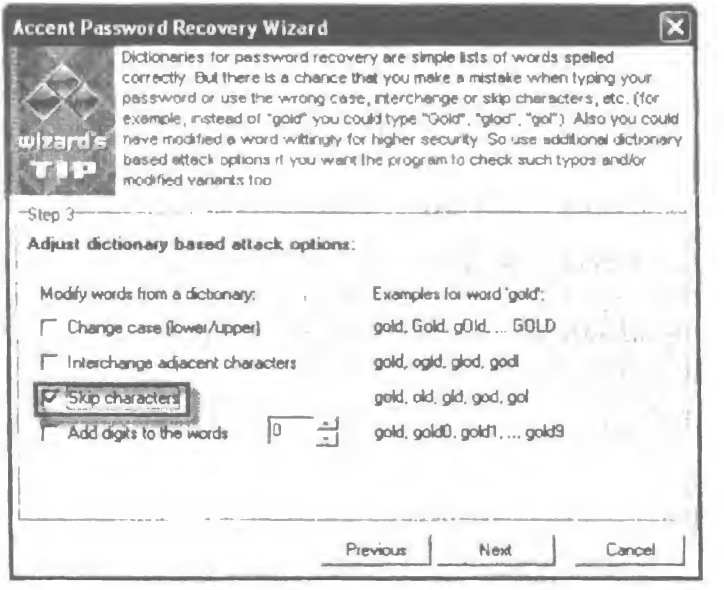
Hình 3.23: *Crack tập tin bằng từ điển.*

3. Tiếp theo, bạn nhấp nút **Add dictionary** để đưa từ điển vào chương trình (xem hình 3.24).



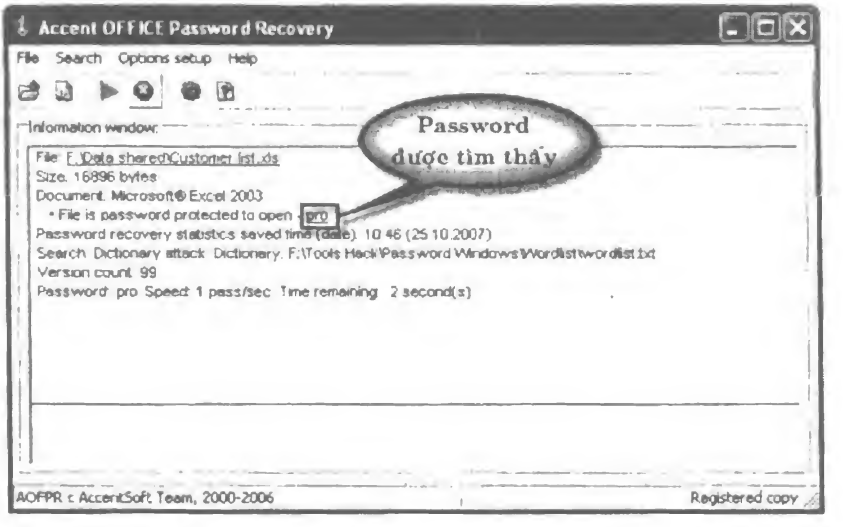
Hình 3.24: *Đưa từ điển vào danh sách.*

4. Tiếp theo, bạn nhấp chọn vào mục **Skip characters** để giữ nguyên trạng thái trong từ điển và nhấp **Next** để tiếp tục (xem hình 3.25).



Hình 3.25: *Giữ nguyên trạng thái trong từ điển.*

5. Sau cùng, nhấp nút **Run search** để thực hiện tìm kiếm. Sau khi quá trình tìm kiếm kết thúc, chương trình sẽ hiển thị thông báo về tình trạng tìm kiếm (xem hình 3.26).



Hình 3.26: *Password được tìm thấy.*

Hướng dẫn thêm:

Bạn có thể sử dụng những phương pháp mà chương trình hỗ trợ để tìm lại password các tập tin, không nhất thiết phải thực hiện các thiết lập mặc định. Trong ví dụ trên ta tách riêng 2 phương pháp ra nhằm tránh tình trạng trùng lặp.

Bạn có thể áp dụng một cách tương tự để tìm password tập tin MS Access (.mdb).

3. Accent Excel Password Recovery

Đây là chương trình được thiết kế nhỏ gọn để tìm password của các tập tin Excel. Tuy có giao diện khiêm tốn, nhưng những thuật toán mà nó xử lý thì rất nhanh. Những password có độ dài nhỏ hơn 5 ký tự có thể được tìm thấy trong khoảng 3 phút.

Sau khi giải nén và cài đặt chương trình, bạn thực hiện tương tự như những phần trước để tìm password.

4. Excel Password Recovery

Đây là chương trình cho phép bạn tìm những password trên các tập tin của MS Excel. Chương trình này có khả năng tìm lại tất cả các loại password, những password ngắn có thể được tìm thấy ngay lập tức.

Sau khi giải nén và cài đặt chương trình, bạn thực hiện như sau:

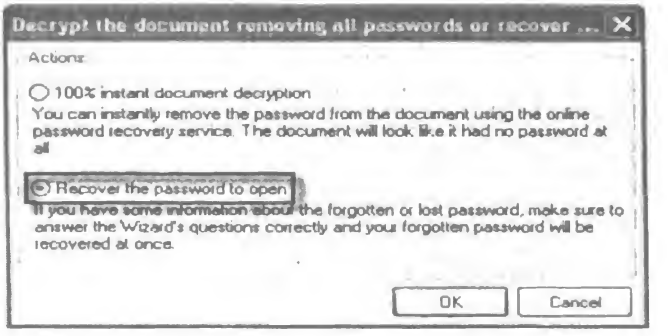
4.1. Tìm password tập tin Excel 97/2000/XP/2003

1. Vào **Start > Programs > Excel Password Recovery > Excel Password Recovery** để mở chương trình.
2. Nhấp nút **Open** để mở file .xls muốn crack, hộp thoại Decrypt the document removing password or recovery xuất hiện.

Ví dụ này sẽ tìm password tập tin Customer list.xls trong thư mục F:\Data share\Customer list.xls.

3. Nhấp chọn **Recover the password to open**. Sau đó nhấp **OK** để mở hộp thoại Create password recovery project.

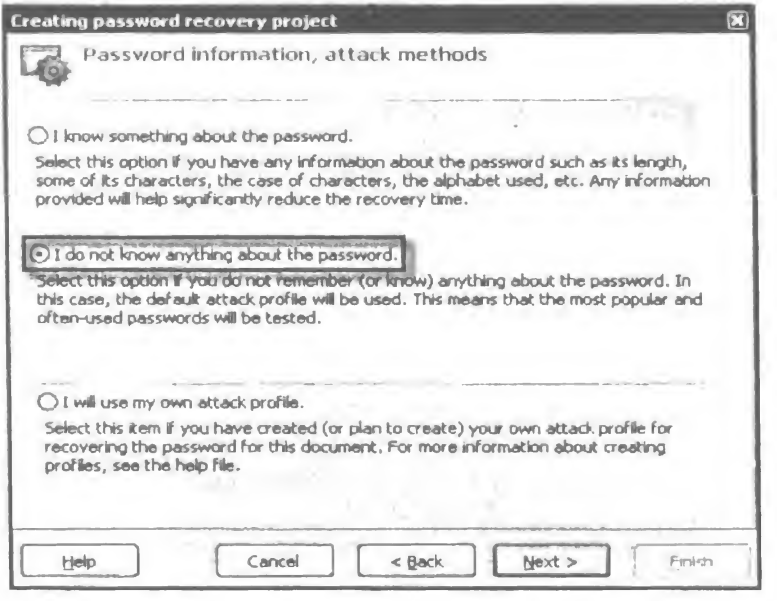
Lựa chọn này có chức năng tìm password của tập tin mà bạn vừa mở (xem hình 3.27).



Hình 3.27: *Tìm password file vừa mở.*

4. Nhấp **Next** để tiếp tục. Sau đó tại mục Password information, attack methods nhấp chọn mục **I do not know anything about the password** và nhấp **Next** để tiếp tục.

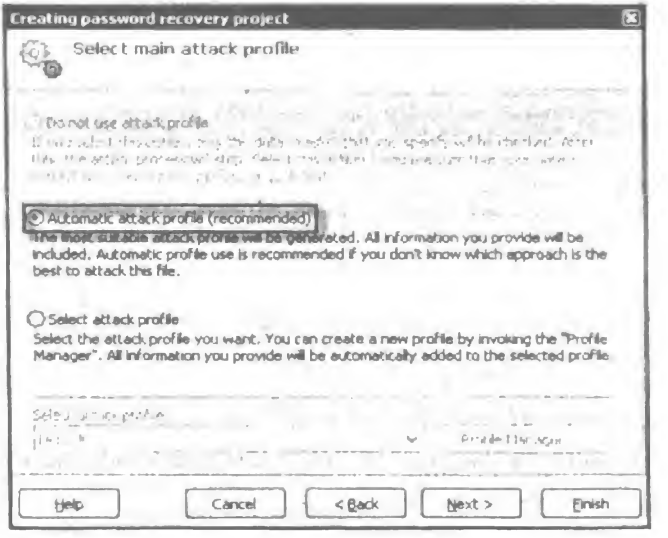
Nếu bạn không biết bất kỳ thông tin nào về password thì lựa chọn này là một giải pháp giúp bạn thực hiện tốt việc dò tìm (xem hình 3.28).



Hình 3.28: *Ủy thác việc tìm password cho chương trình.*

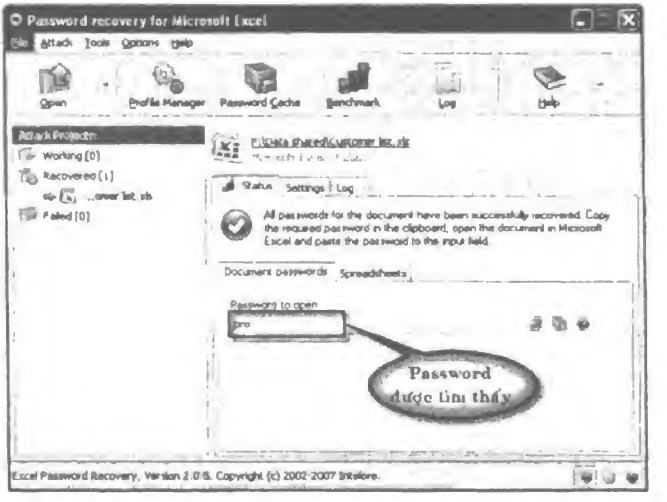
5. Tiếp theo, nhấp chọn mục **Automatic attack profile (recommended)**, nhấp **Next** để tiếp tục.

Mục này được chọn, chương trình sẽ tự tìm những profile thích hợp để tìm (xem hình 3.29).



Hình 3.29: *Chương trình tự gán profile thích hợp.*

6. Tiếp theo, bạn nhấp **Finish** để thực hiện. Sau khi quá trình xử lý kết thúc, chương trình sẽ hiển thị password (xem hình 3.30).



Hình 3.30: *Password được tìm thấy.*

4.2. Tìm password MS Excel 2007

Bộ Office 2007 ra đời với nhiều cải tiến và giao diện tương đối đẹp mắt, hơn nữa những phần mềm của nó cũng trực quan và dễ sử dụng. Ngoài ra, nó còn được biết đến với tính bảo mật tương đối cao.

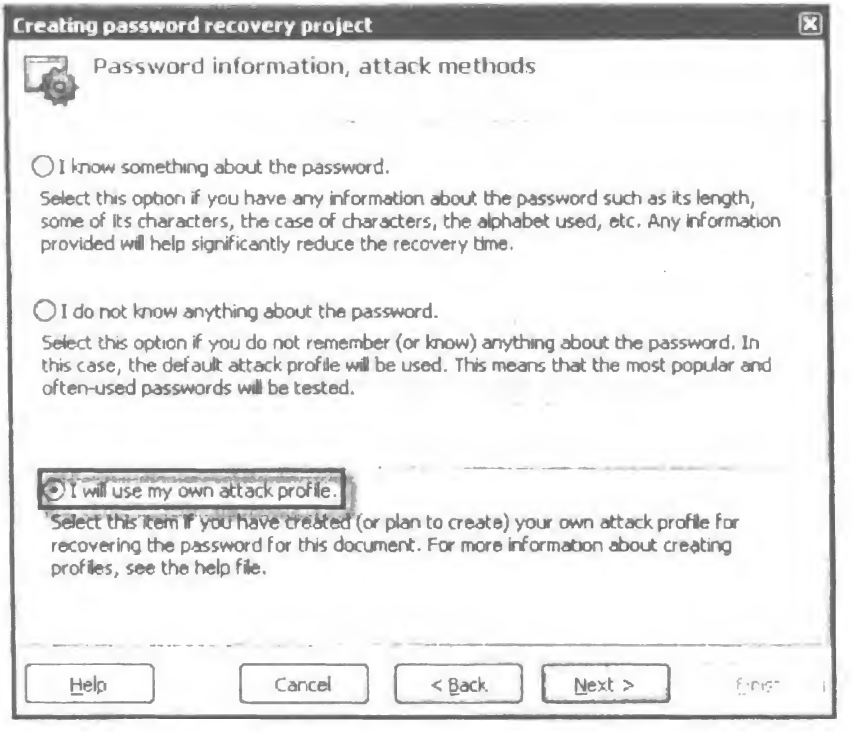
Những tập tin mà Excel 2007 lưu mặc định sẽ có định dạng .xlsx.

Ví dụ, tìm password tập tin userlist.xlsx tại thư mục F:\Data shared\userlist.xlsx, để thực hiện bạn làm như sau:

1. Nhấp nút **Open** để mở tập tin có định dạng .xlsx muốn tìm password. Hộp thoại Create password recovery project xuất hiện, nhấp **Next** để tiếp tục.

2. Tiếp theo, bạn nhấp chọn vào mục **I will use my own attack profile**, sau đó nhấp **Next** để tiếp tục.

Mục này cho phép bạn chọn một profile nhất định để thực hiện attack (xem hình 3.31).

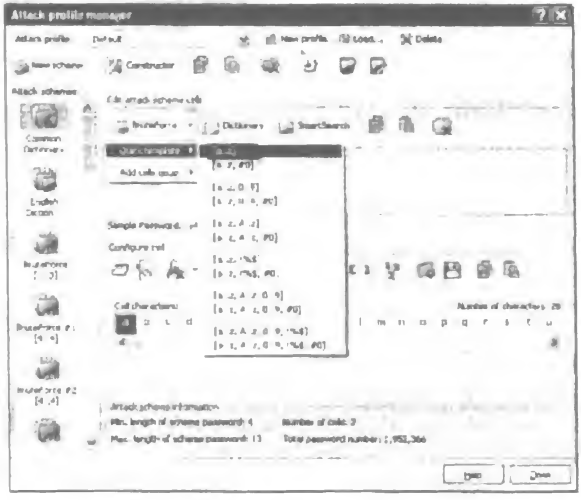


Hình 3.31: *Chọn profile mà bạn muốn sử dụng.*

3. Tiếp theo, bạn nhấp nút **Profile Manager** để mở một profile của chương trình.

4. Nhấp chọn **Brute-force > Quick template > [a..z]** để crack theo kiểu Brute-force. Sau đó, nhấp **Close** để áp dụng (xem hình 3.32).

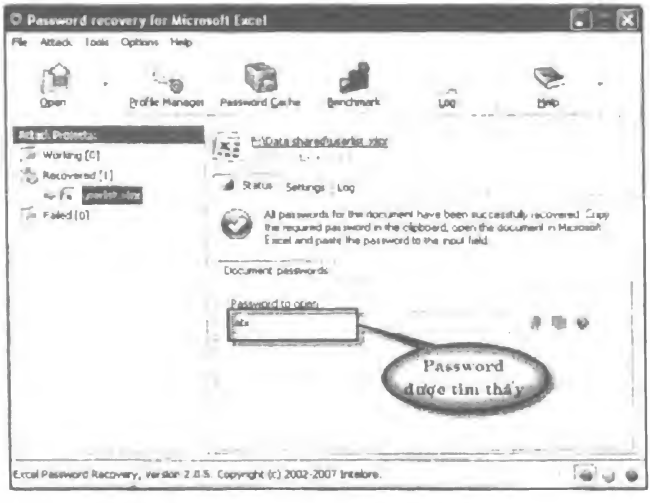
5. Sau cùng, nhấp **Finish** để thực hiện.



Hình 3.32: *Crack bằng phương pháp Brute-force.*

6. Sau khi xử lý thành công, chương trình sẽ hiển thị password trong giao diện chính của chương trình (xem hình 3.33).

Bạn có thể áp dụng cách tương tự để tìm password trên các tập tin của MS Excel 2003, không nhất thiết phải theo sự phân chia như mục trên. Các mục hoàn toàn có thể hoán đổi cho nhau.



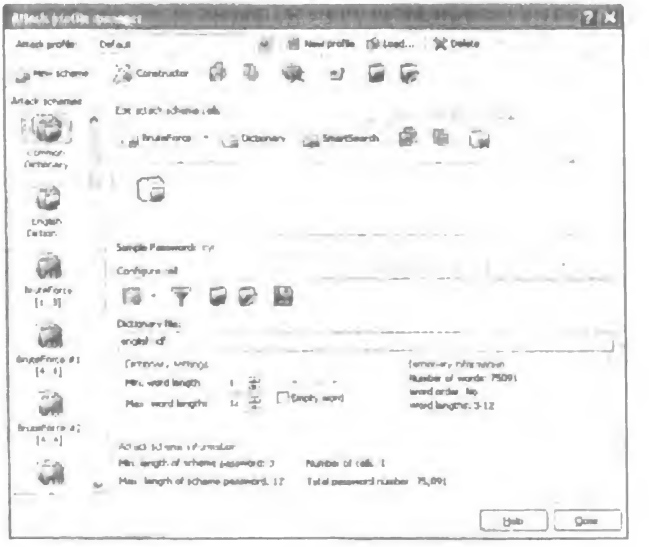
Hình 3.33: *Password được tìm thấy.*

4.3. Phương pháp tạo từ điển trên Excel Password Recovery

Không như những chương trình tìm kiếm password khác, bạn có thể tạo từ điển từ tập tin văn bản. Chương trình này tích hợp sẵn những

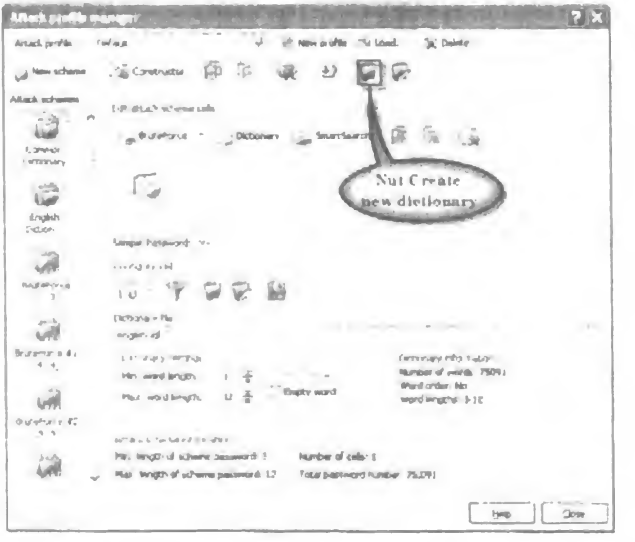
mục cần thiết để bạn có thể tạo từ điển ngay trên chương trình. Để từng bước tạo từ điển, bạn thực hiện như sau:

1. Ngay trên giao diện chính của chương trình, bạn nhấp mục **Profile Manager** để mở hộp thoại Attack profile manager (xem hình 3.34)



Hình 3.34: *Mở hộp thoại Attack profile manager.*

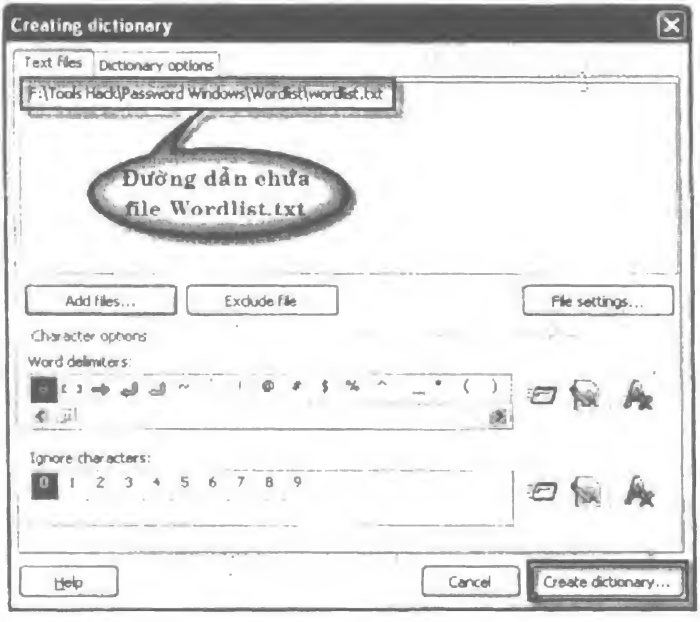
2. Tiếp theo, nhấp nút **Create new dictionary** để mở hộp thoại Creating dictionary (xem hình 3.35)



Hình 3.35: *Nhấp nút Create new dictionary.*

3. Trong hộp thoại Creating dictionary, tại thẻ Text files, bạn nhấp nút **Add files** để đưa file có định dạng **.txt** hay **.dic** làm từ điển.

4. Tiếp theo, nhấp nút **Create dictionary**, nhập tên của từ điển để lưu, ví dụ **DictionaryVNCS.ldf** (xem hình 3.36).



Hình 3.36: *Tạo file từ điển từ file text.*

5. MS Outlook Password Recovery

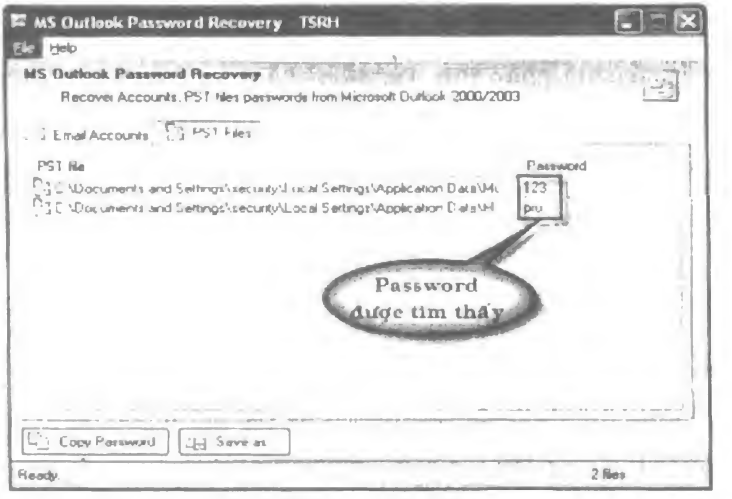
Đây là chương trình cho phép bạn xác định password các tập tin .pst của Outlook Express. Giao diện của chương trình rất đơn giản và dễ sử dụng. Password của tập tin có thể được tìm thấy và hiển thị ngay trên giao diện chính của chương trình.

Sau khi giải nén và cài đặt chương trình vào máy tính, bạn thực hiện như sau:

1. Vào **Start > Programs > MS Outlook Password Recovery > MS Outlook Password Recovery** để mở chương trình.

2. Khi chương trình được khởi chạy, bạn phải đợi khoảng 3 phút để chương trình thực hiện tìm kiếm.

3. Password cùng nhiều thông tin được hiển thị ngay trên giao diện chính của chương trình (xem hình 3.37).



Hình 3.37: *Password được tìm thấy.*

V. Tìm password các tập tin của Adobe Acrobat Reader (pdf)

Trong mục này sẽ giới thiệu một số phần giúp tìm lại password trên những tập tin có định dạng .pdf.

1. PDF Password Cracker Pro V.3.0

Đây là chương trình cho phép tìm lại password tập tin .pfd. Sau khi giải nén và cài đặt chương trình, bạn thực hiện như sau:

1.1. Tìm password theo phương pháp Brute-force

Phương pháp này cho phép tìm nhanh những password có độ dài nhỏ hơn 5 kỷ tự. Hơn nữa, những thiết lập trong mục này cũng khá đơn giản.

Ví dụ, tìm password của tập tin Security document.pdf ở thư mục F:\Data shared\Security document.pdf. Để thực hiện, bạn làm như sau:

1. Vào **Start > Programs > PDF Password Cracker Pro v3.0 > PDF Password Cracker Pro v3.0** để mở chương trình.
2. Tại giao diện chính của chương trình, bạn nhấp nút **Load** để mở tập tin .pdf muốn tìm password.

Ví dụ, tìm password tập tin Security document.pdf trong thư mục F:\Data shared\Security document.pdf.

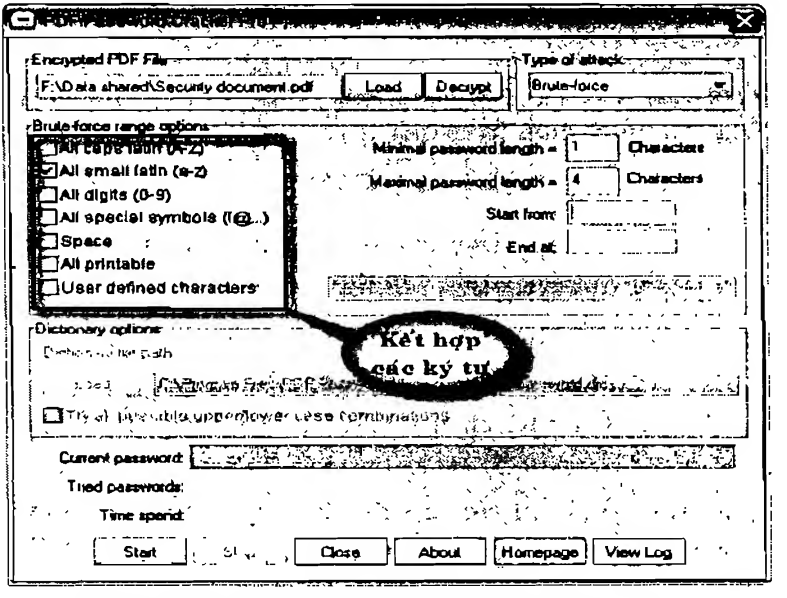
3. Tiếp theo, trong mục Type of attack, bạn nhấp chọn Brute-force.

Đây là phương pháp tìm password bằng cách kết hợp các ký tự cho trước.

4. Tại mục Brute-force range options, bạn tham khảo các lựa chọn sau:

- **All caps latin [A-Z]:** Tất cả các ký tự Latin hoa từ A – Z.
- **All small latin [a-z]:** Các ký tự Latin thường từ a – z.
- **All digits [0-9]:** Tất cả các ký tự số từ 0 – 9.
- **All special simbols [!@...]:** Tất cả các ký tự đặc biệt.
- **User defined characters:** Ký tự do người dùng định nghĩa.

5. Nhập vào độ dài nhỏ nhất cho chuỗi password trong mục **Minimal password length**, mặc định là 1 và **Maximal password length**, độ dài lớn nhất cho chuỗi password (xem hình 3.38).



Hình 3.38: *Những thiết lập trong mục Brute-force.*

6. Nhấp nút **Start** để bắt đầu tìm kiếm. Sau khi xử lý xong, chương trình sẽ xuất hiện hộp thoại yêu cầu bạn lưu nội dung tập tin mà nó đã crack được. Bạn nhập tên tập tin cần lưu, tiếp theo nhấp **OK** để hoàn thành. Sau khi xử lý xong, chương trình hiển thị password trên giao diện chính của chương trình (xem hình 3.39).

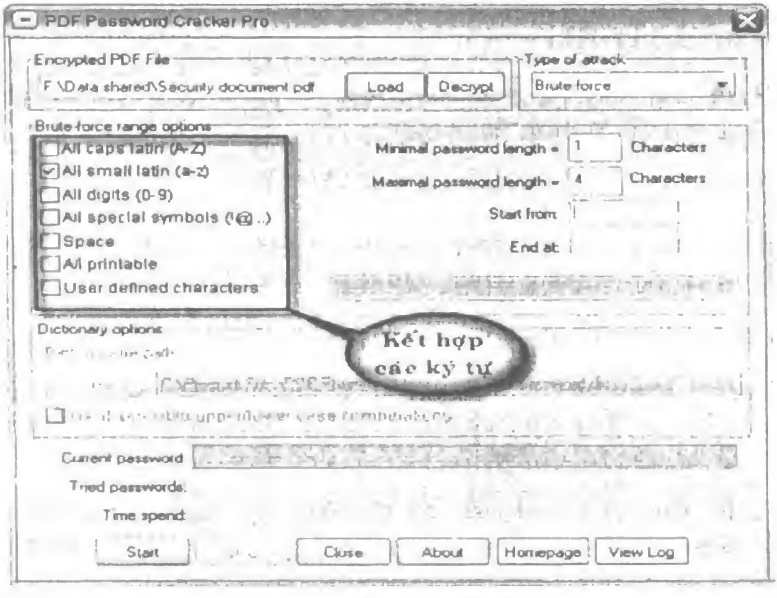
3. Tiếp theo, trong mục Type of attack, bạn nhấp chọn Brute-force.

Đây là phương pháp tìm password bằng cách kết hợp các ký tự cho trước.

4. Tại mục Brute-force range options, bạn tham khảo các lựa chọn sau:

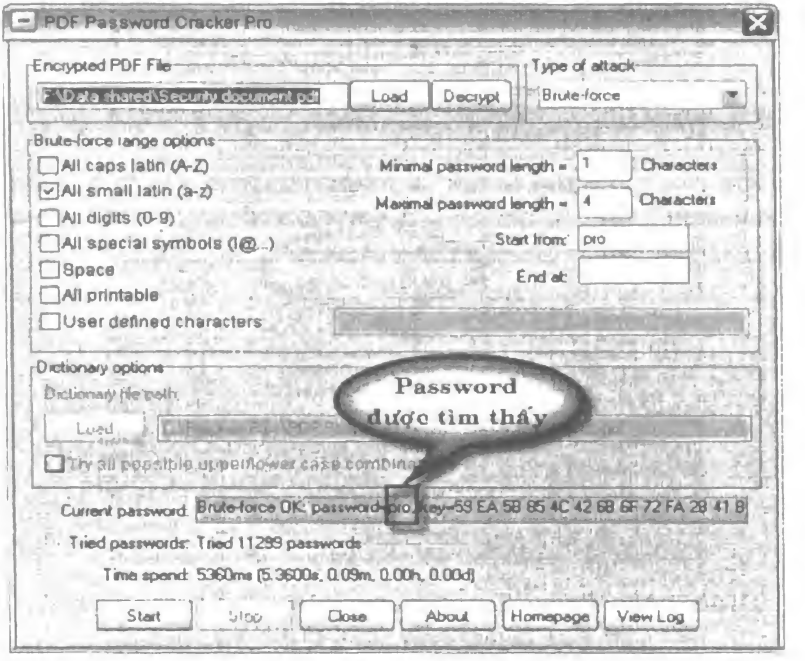
- **All caps latin [A-Z]:** Tất cả các ký tự Latin hoa từ A – Z.
- **All small latin [a-z]:** Các ký tự Latin thường từ a – z.
- **All digits [0-9]:** Tất cả các ký tự số từ 0 – 9.
- **All special simbols [!@...]:** Tất cả các ký tự đặc biệt.
- **User defined characters:** Ký tự do người dùng định nghĩa.

5. Nhập vào độ dài nhỏ nhất cho chuỗi password trong mục **Minimal password length**, mặc định là 1 và **Maximal password length**, độ dài lớn nhất cho chuỗi password (xem hình 3.38).



Hình 3.38: *Những thiết lập trong mục Brute-force.*

6. Nhấp nút **Start** để bắt đầu tìm kiếm. Sau khi xử lý xong, chương trình sẽ xuất hiện hộp thoại yêu cầu bạn lưu nội dung tập tin mà nó đã crack được. Bạn nhập tên tập tin cần lưu, tiếp theo nhấp **OK** để hoàn thành. Sau khi xử lý xong, chương trình hiển thị password trên giao diện chính của chương trình (xem hình 3.39).



Hình 3.39: *Password được tìm thấy.*

1.2. Tìm password bằng phương pháp từ điển

Trong mục này vẫn sử dụng từ điển là file Wordlist.txt. Các bước thực hiện như sau:

1. Nhấp nút **Load** để mở tập tin .pdf muốn tìm password.

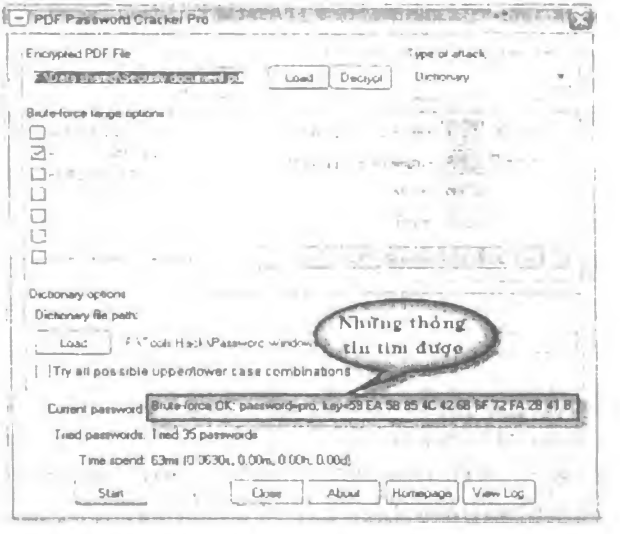
Ví dụ sử dụng phương pháp này để crack password tập tin Security document.pdf trong thư mục F:\Data shared\ Security document.pdf.

2. Tiếp theo, bạn nhấp nút **Load** trong mục Dictionary options để đưa từ điển vào chương trình, trong ví dụ này là file Wordlist.txt. Sau đó, bạn nhấp chọn vào mục **Try all possible upper/lower case combinations** (kết hợp chữ hoa và chữ thường) (xem hình 3.40).

3. Nhấp nút **Start** để thực hiện. Sau khi hoàn thành, chương trình sẽ yêu cầu bạn nhập tên và đường dẫn lưu tập tin.

Tập tin này sẽ không có password. Đây là tập tin sao lưu của tập tin mà ta đã loại bỏ password. Nếu không muốn sao lưu tập tin này thì bạn có thể nhấp nút **Cancel**. Tiếp theo, password được hiển thị ngay trên giao diện chính của chương trình (xem hình 3.41).

Hình 3.40: *Những thiết lập của phương pháp dictionary.*



Hình 3.41: *Những thông tin tìm được.*

Ngoài ra, chương trình còn hỗ trợ thêm một số chức năng khác như Key search. Bạn có thể khám phá thêm khi sử dụng chương trình.

2. Advanced PDF Password Recovery Pro V.2.0.4

Đây là một chương trình tìm password tập tin .pdf chuyên nghiệp. Nó có thể tìm được password trên những files của Adobe Acrobat Reader bằng nhiều phương pháp.

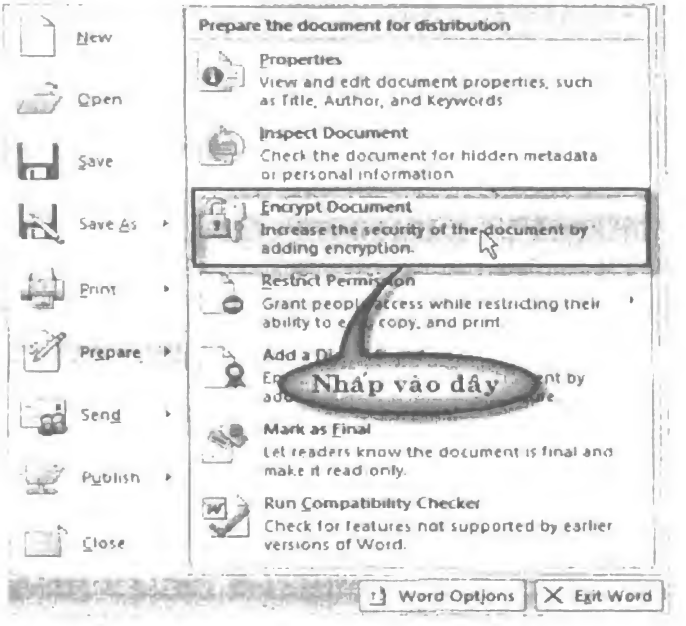
Giao diện thân thiện, cách sử dụng trực quan, những thiết lập tương đối dễ dàng, từ điển mở. Sau khi giải nén và cài đặt thành công chương trình, bạn thực hiện tương tự như cách trên để tìm password.

VI. Đặt password cho tập tin

1. Đặt password cho những tập tin của MS Word 2007

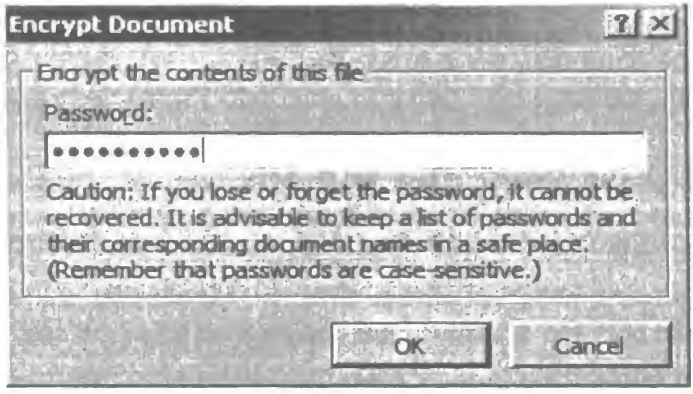
Một phương pháp bảo vệ hữu hiệu cho các tài liệu của MS Word là đặt password truy cập tập tin. Phương pháp thực hiện như sau:

1. Vào **Start > Programs > Microsoft Office > Microsoft Office Word 2007** để mở MS Word.
2. Mở tập tin muốn đặt password. Sau đó bạn nhấp nút **Office Button** để mở menu.
3. Tiếp theo, vào **Prepare > Encypt Document** để mở hộp thoại Encrypt Document (xem hình 3.42).



Hình 3.42: *Chọn Encrypt Document.*

4. Tại hộp thoại này, bạn nhập password vào ô **Password**, sau đó nhấp **OK** để tiếp tục (xem hình 3.43).



Hình 3.43: *Nhập password.*

5. Bạn nhập lại password trong mục Reenter password. Sau đó, bạn lưu tập tin này lại.

Để kiểm tra, bạn mở tập tin vừa lưu, lúc này chương trình sẽ yêu cầu password (xem hình 3.44).

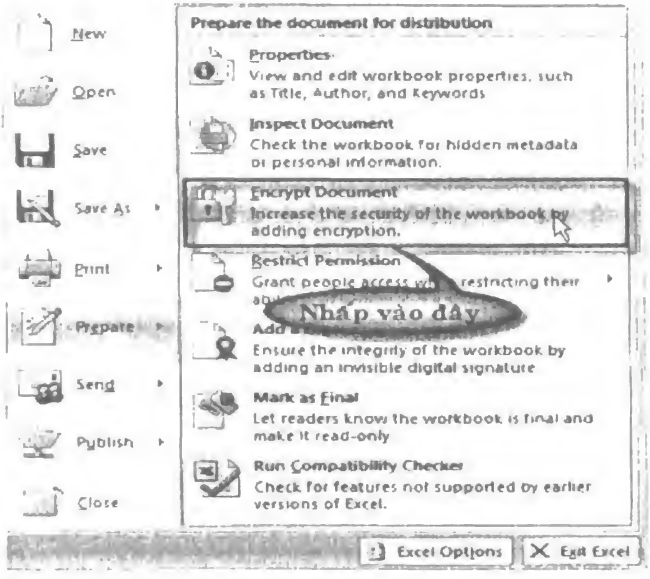
Hình 3.44: *Nhập lại password.*

2. Đặt password cho các tập tin của MS Excel 2007

1. Vào **Start > Programs > Microsoft Office > Microsoft Office Excel 2007** để mở MS Excel.

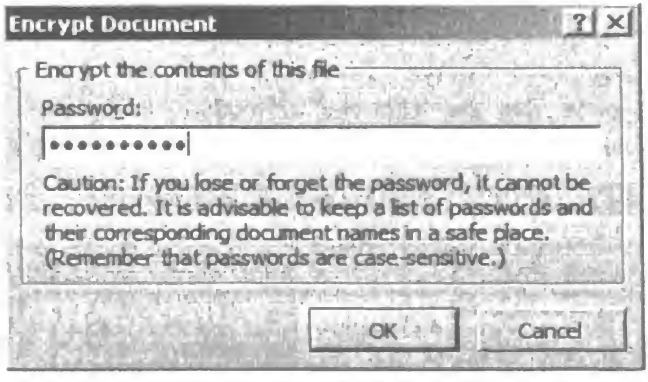
2. Tiếp theo, mở tập tin muốn đặt password. Sau đó nhấp nút **Office Button** để mở menu.

3. Vào menu **Prepare > Encrypt Document** để mở hộp thoại Encrypt Document (xem hình 3.45).



Hình 3.45: *Chọn Encrypt Document.*

4. Tại hộp thoại Encrypt Document bạn nhập vào **password** mà bạn muốn đặt cho tập tin, tiếp theo, nhấp **OK** và nhập lại password vào mục **Reenter password** (xem hình 3.46).



Hình 3.46: *Nhập password cho tập tin Excel.*

5. Tiếp theo, bạn nhấn tổ hợp phím **Ctrl + S** để lưu lại những thông này vào tập tin.

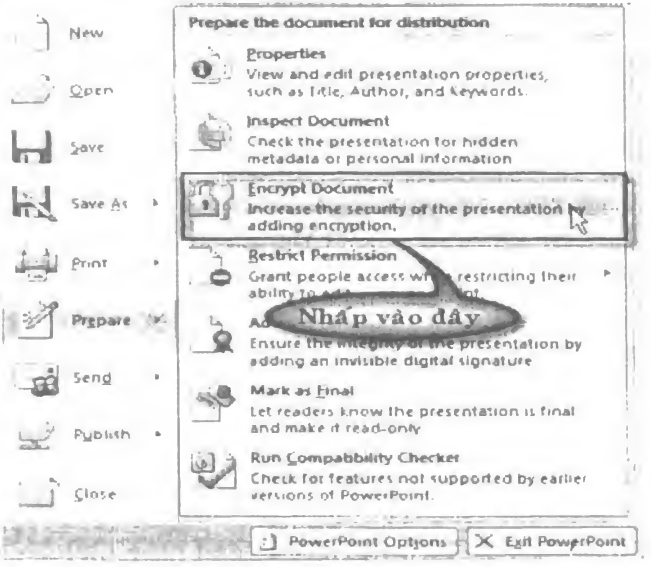
Như vậy là hoàn thành việc đặt password cho tập tin.

3. Đặt password cho các tập tin của MS PowerPoint 2007

1. Vào **Start > Programs > Microsoft Office > Microsoft Office PowerPoint 2007** để mở MS PowerPoint 2007.

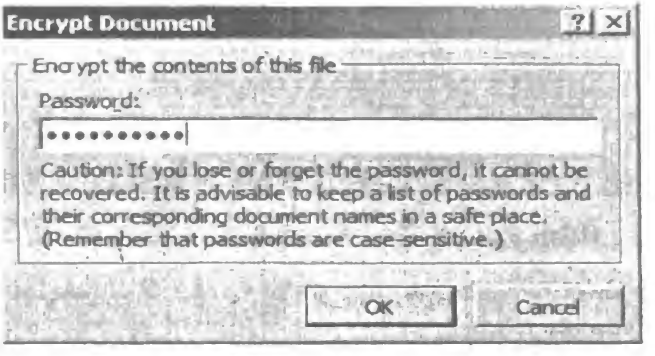
2. Tiếp theo, mở tập tin muốn đặt password, sau đó nhấp nút **Office Button** để mở menu.

3. Tiếp theo, vào menu **Prepare > Encrypt Document** để mở hộp thoại Encrypt Document (xem hình 3.47).



Hình 3.47: *Chọn Encrypt Document.*

4. Tại hộp thoại Encrypt Document bạn nhập vào **password** mà bạn muốn đặt cho tập tin, tiếp theo, nhấp **OK** và nhập lại password vào mục **Reenter password** (xem hình 3.48).



Hình 3.48: *Nhập password cho tập tin của Excel.*

5. Tiếp theo, bạn nhấn tổ hợp phím **Ctrl + S** để lưu lại những thông này vào tập tin.

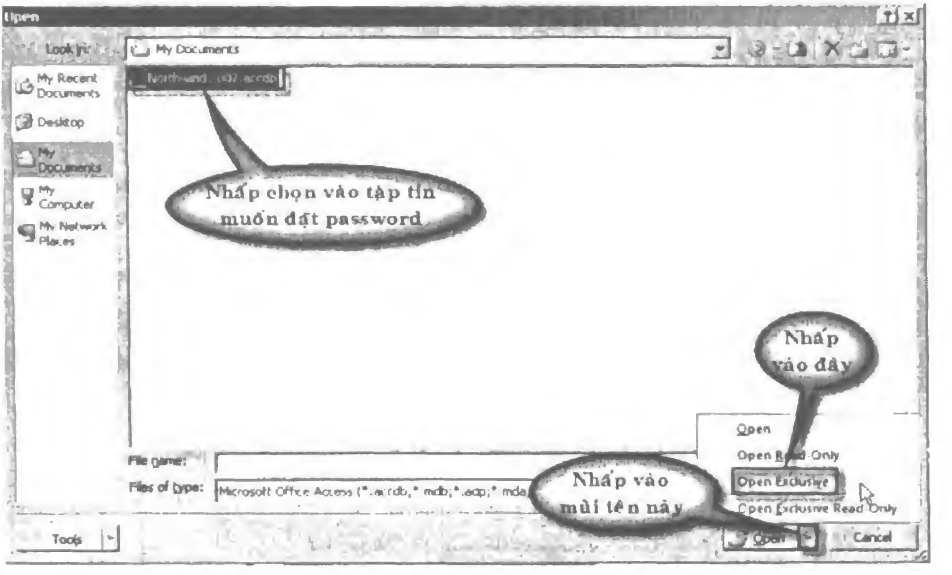
Như vậy là bạn đã hoàn thành việc đặt password cho tập tin.

4. Đặt password cho các tập tin của MS Access 2007

Cũng tương tự như các mục trước, để bảo vệ tập tin thì phương pháp đặt password là rất hiệu quả. Để thực hiện, bạn làm như sau:

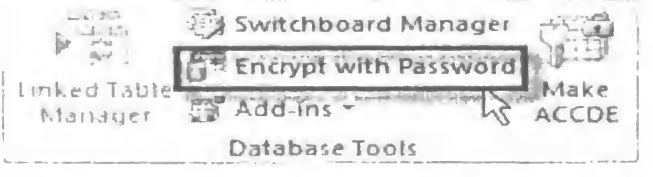
1. Vào **Start > Programs > Microsoft Office > Microsoft Office Access 2007** để mở MS Access 2007.

2. Tiếp theo, nhấp nút **Office Button** > **Open**, sau đó tại hộp thoại Open, bạn nhấp chọn vào tập tin mà bạn muốn đặt password, tiếp thep nhấp vào mũi tên ở nút **Open**, chọn Open Exclusive (xem hình 3.49).



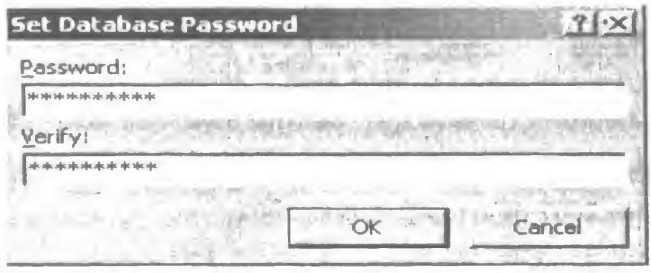
Hình 3.49: *Mở tập tin muốn đặt password.*

3. Tiếp theo, chọn thẻ **Database Tools**, sau đó chọn mục **Encrypt with Password** (xem hình 3.50).



Hình 3.50: *Chọn Encrypt with Password.*

4 Tiếp theo, bạn nhập password và nhập lại password trong hộp thoại Set Database Password, sau cùng nhấp **OK** để hoàn thành (xem hình 3.51).

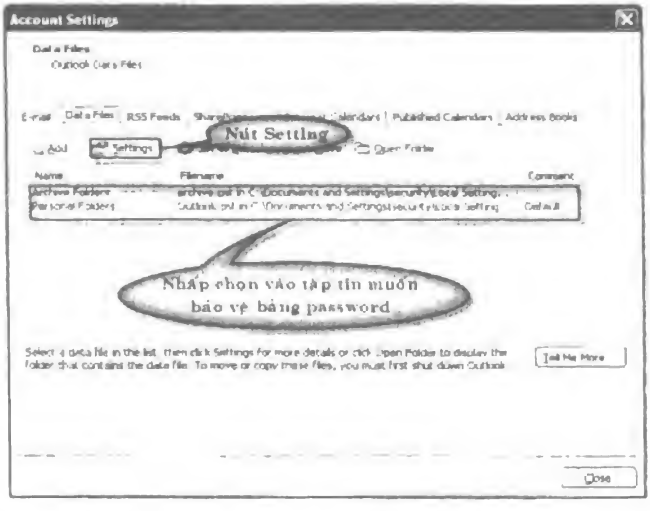


Hình 3.51: *Nhập password cho cơ sở dữ liệu.*

5. Đặt password cho tập tin .pst của MS Outlook Express 2007

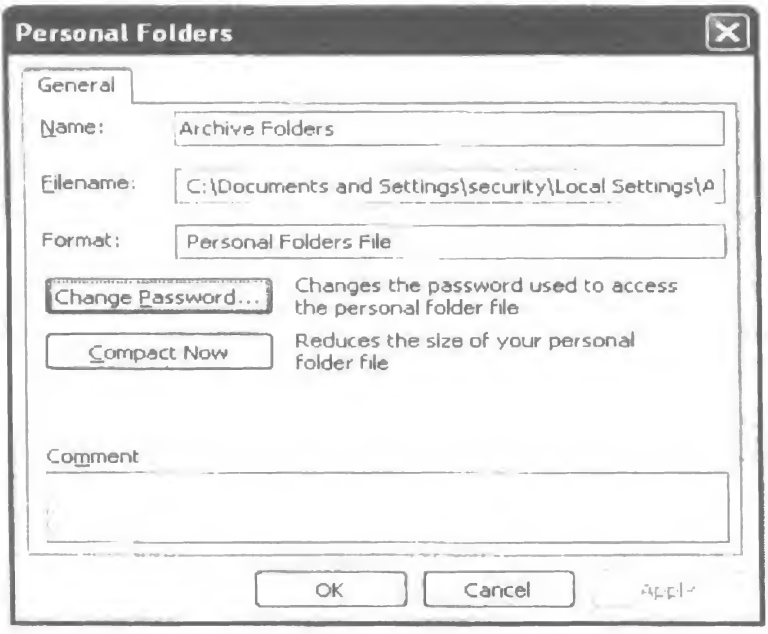
Để bảo vệ những thông tin cá nhân được lưu trong e-mail, mà những thông tin này thường chứa trong tập tin .pst được quản lý bằng MS Outlook Express 2007 Để thực hiện, bạn làm như sau:

1. Vào **Start > Programs > Microsoft Office > Microsoft Office Outlook 2007** để mở Microsoft Office Outlook 2007.
2. Tiếp theo, bạn vào menu **File > Data File Management** để mở hộp thoại **Account Settings**.
3. Tại thẻ Data Files, bạn nhấp chọn vào tập tin muốn bảo vệ bằng password, sau đó nhấp nút **Settings** (xem hình 3.52).



Hình 3.52: *Các mục trong hộp thoại Account Settings.*

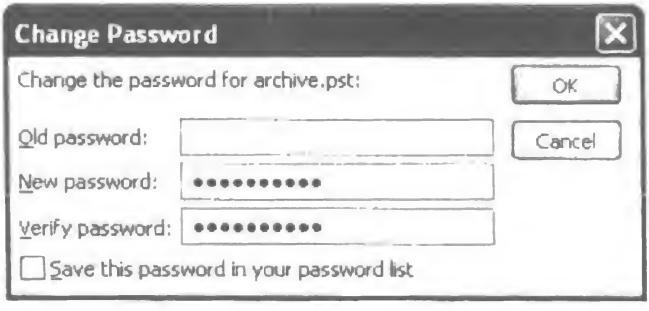
4. Sau khi nhấp nút Settings, hộp thoại Personal Folders xuất hiện (xem hình 3.53).



Hình 3.53: *Hộp thoại Personal.*

5. Nhấp nút **Change Password** để mở hộp thoại Change Password, tiếp theo bạn nhập password trong mục **New password** và nhập lại password trong mục **Verify password**, sau đó nhấp **OK** để áp dụng.

Mục **Old password** bỏ trống nếu bạn đặt password lần đầu (xem hình 3.54).



Hình 3.54: *Nhập password cho tập tin .pst.*

6. Đặt password cho tập tin của Winzip và Winrar

Để bảo vệ các tập tin nén của chúng ta thì phương pháp đặt password luôn là giải pháp hữu dụng. Để thực hiện được điều này, bạn phải có ít nhất một trong hai chương trình đó là Winzip hoặc Winrar.

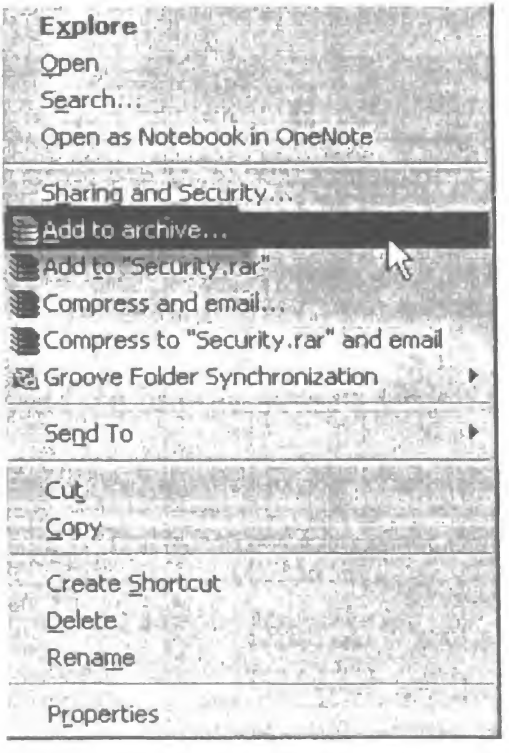
Mục này sẽ giới thiệu đến các bạn phương pháp đặt password cho tập tin của Winzip và Winrar bằng chương trình Winrar 4.65. Chương trình được cung cấp trong thư mục Genaral Software.

6.1. Đặt password cho tập tin của Winzip

Tập tin của Winzip thường có phần mở rộng là .zip, trong ví dụ này chúng ta sẽ sử dụng Winrar để đặt password cho tập tin của Winzip.

Ví dụ: Bạn có một thư mục có tên là Security được lưu ở thư mục gốc của ổ đĩa D trên máy tính. Để nén thư mục đồng thời đặt password cho nó bạn thực hiện như sau:

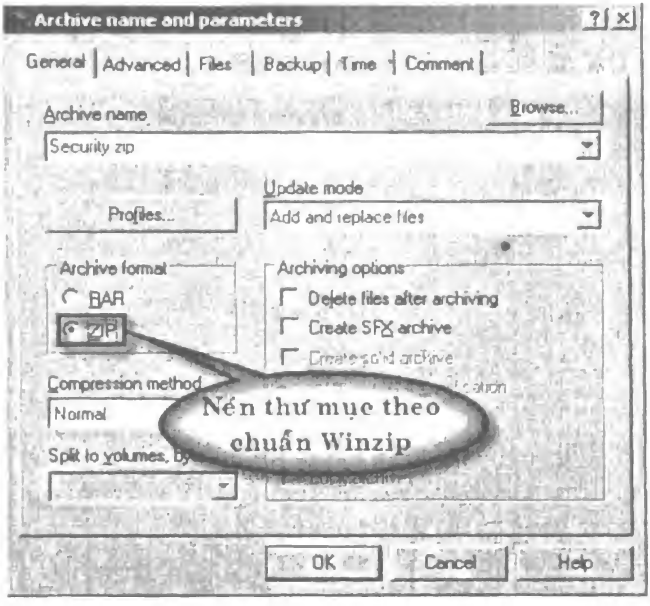
1. Di chuyển vào ổ đĩa **D**, tiếp theo, nhấp phải chuột vào thư mục **Security > Add to archive** (xem hình 3.55).



Hình 3.55: *Chọn Add to archive.*

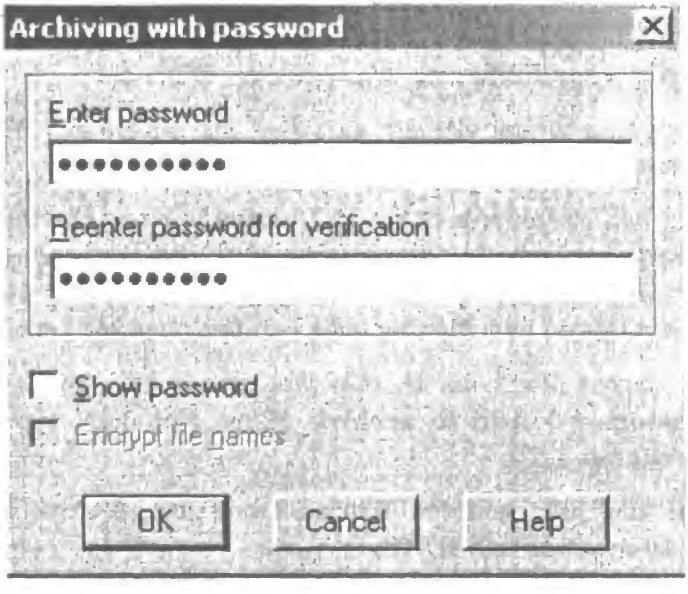
Giao diện của Winrar xuất hiện.

2. Trong mục Archive format, bạn nhấp chọn vào mục **ZIP** để nén tập thư mục này thành Security.zip (xem hình 3.56).



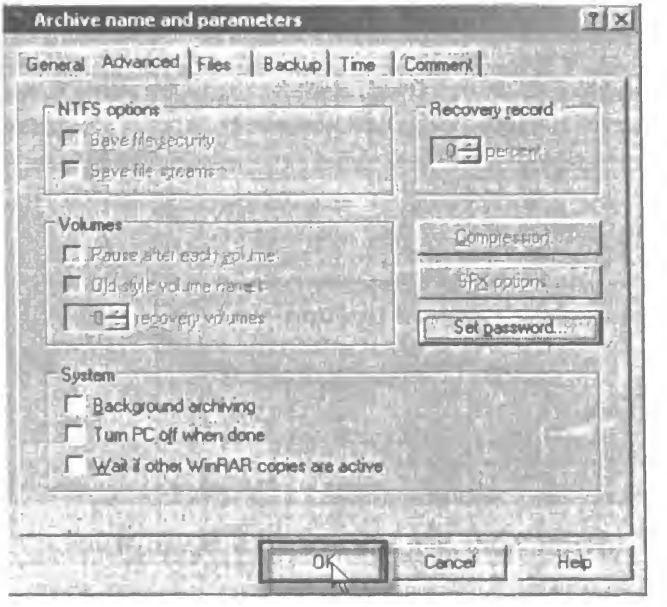
Hình 3.56: *Nén thư mục theo chuẩn Winzip.*

3. Chọn thẻ **Advanced**, nhấp nút **Set password** để mở hộp thoại Archiving with password, tiếp theo, bạn nhập password trong mục **Enter password** và nhập lại password trong mục **Reenter password for verification** (xem hình 3.57)



Hình 3.57: *Nhập password cho tập tin Security.zip.*

4. Tiếp theo trong hộp thoại **Archive name and parameters**, bạn nhấp **OK** để áp dụng (xem hình 3.58).



Hình 3.58: *Nhấp OK để áp dụng.*

Như vậy đến đây ta đã hoàn thiện việc nén thư mục Security thành tập tin Security.zip và đặt password. Khi giải nén cũng như truy cập vào tập tin này, chương trình sẽ luôn yêu cầu bạn phải nhập password.

6.2. Đặt password cho các tập tin của Winrar

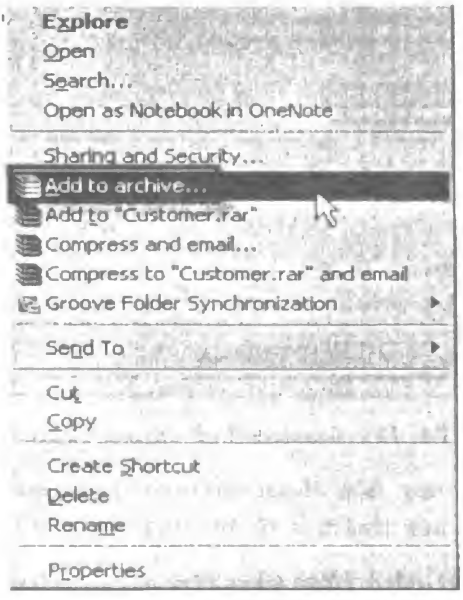
Cũng tương tự như việc đặt password cho tập tin của Winzip, trong mục này chúng ta cũng sử dụng Winrar để thực hiện.

Ví dụ bạn có thư mục có tên là **Customer** trong thư mục gốc của ổ đĩa **D** lưu trữ những tài liệu về thông tin khách hàng của công ty. Do thư mục này chiếm dung lượng khá lớn nên bạn muốn nén lại đồng thời đặt password cho tập tin này. Để thực hiện bạn làm theo các bước sau:

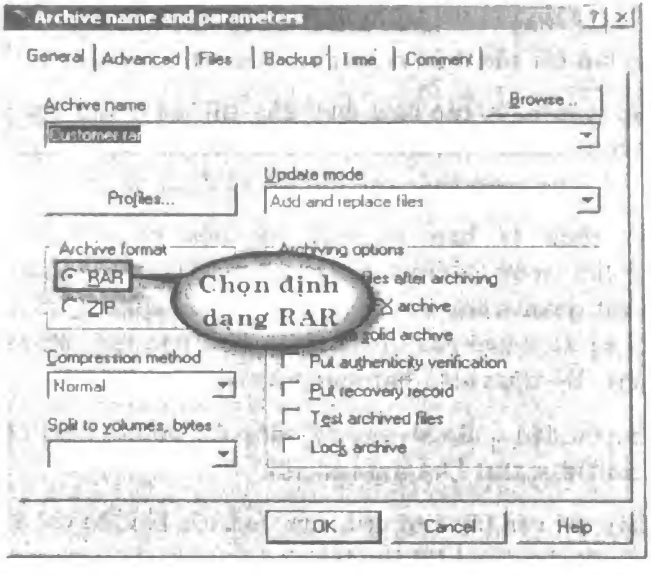
1. Di chuyển đến ổ đĩa **D**, tiếp theo nhấp phải chuột vào thư mục **Customer > Add to archive** để mở giao diện nén của Winrar (xem hình 3.59).

2. Tại giao diện nén của Winrar, trong mục Archive format, bạn nhấp chọn vào mục **RAR**.

Định dạng này có chức năng nén thư mục Customer thành tập tin Customer.rar (xem hình 3.60).

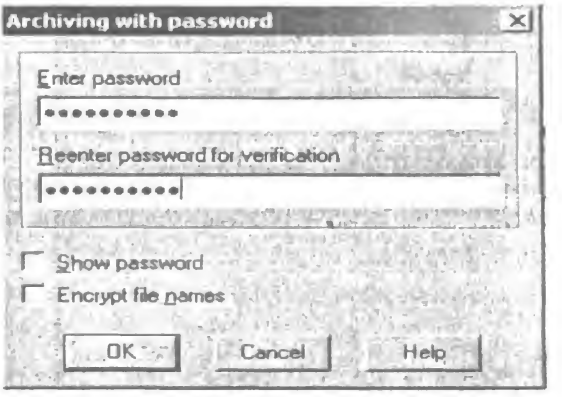


Hình 3.59: *Chọn Add to archive.*



Hình 3.60: *Nén thư mục thành định dạng RAR.*

3. Chọn thẻ **Advanced**, tiếp theo nhấp nút **Set password** để mở hộp thoại Archiving with password. Bạn nhập password trong mục **Enter password** và nhập lại password trong mục **Reenter password for verification**, sau đó nhấp **OK** để áp dụng (xem hình 3.61).



Hình 3.61: *Đặt password cho tập tin của Winrar.*

4. Tiếp theo, trong hộp thoại Archive name with parameters, bạn nhấp **OK** để nén thư mục và áp dụng password.

7. Đặt password cho các tập tin của Adobe Acrobat Reader (pdf)

Trong mục này sẽ giới thiệu cùng các bạn phương pháp đặt password cho tập tin của Adobe Acrobat Reader có phần mở rộng là PDF.

Để thực hiện được các mục dưới đây thì máy tính của bạn phải cài đặt chương trình Adobe Acrobat 7.0 Professional. Đây là phần mềm cho phép bạn vừa đọc và soạn thảo các tập tin có định dạng .pdf.

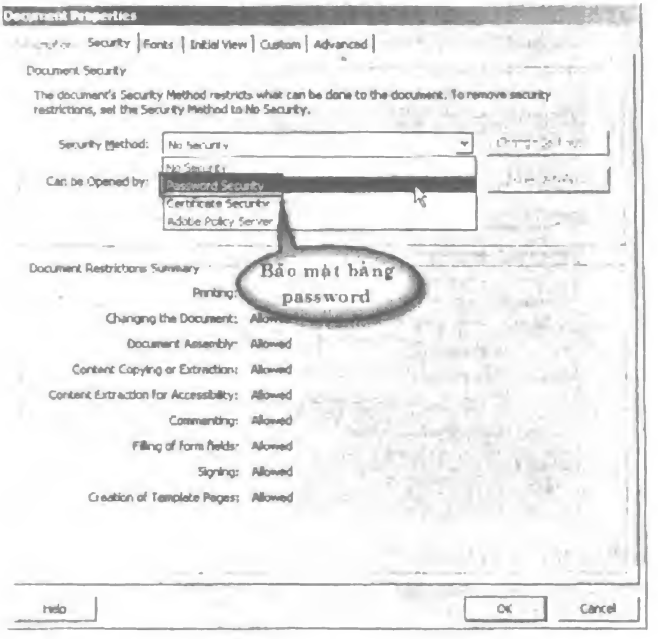
Giả sử công ty bạn có một tài liệu có tên là Confidential Document.pdf lưu trong thư mục gốc của ổ đĩa D. Tài liệu này chứa những dữ liệu mật, rất quan trọng được định dạng theo chuẩn pdf. Để bảo vệ tài liệu này khỏi sự dòm ngó của người khác, bạn nên đặt password truy cập cho tập tin này. Để thực hiện bạn làm như sau:

1. Di chuyển đến ổ đĩa **D**, sau đó nhấp đôi vào tập tin này để mở tập tin **Confidential Document.pdf**.

Khi nhấp đôi vào tập tin, nếu máy tính của bạn đã cài đặt phần mềm Adobe Acrobat Professional thì tập tin sẽ được mở bởi chương trình này.

2. Tại giao diện chính của chương trình, vào menu **File > Document Properties**, hộp thoại Document Properties xuất hiện.

3. Tại hộp thoại Document Properties, bạn chọn thẻ **Security**, tiếp theo trong mục Security Method, chọn **Password security** (xem hình 3.62).



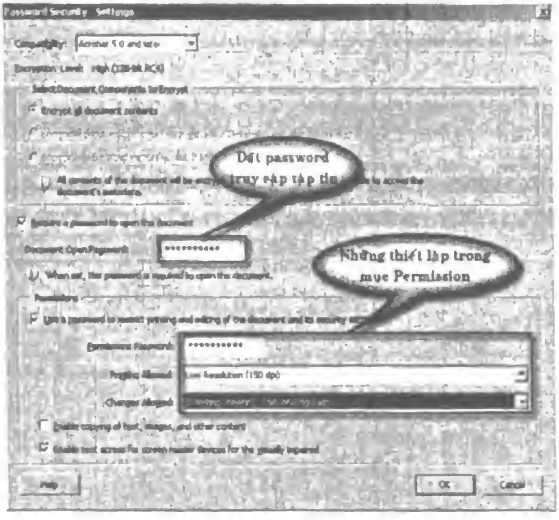
Hình 3.62: *Những thiết lập tại mục Password security.*

4 Tiếp theo, bạn nhấp chọn vào mục **Require a password to open the document**, sau đó nhập password vào mục Document Open Password.

5 Trong mục Permission, bạn thiết lập như sau:

- Nhấp chọn vào mục **Use a password to restrict printing and editing of the document and its security setting** (sử dụng password để hạn chế in và soạn thảo tài liệu).
- **Permission password:** Bạn nhập password cho sự ủy quyền.
- **Printing allowed:** Chọn Low Resolutions (150 dpi) để cho phép in ở chế độ phân giải thấp.
- **Change allowed:** Chọn Inserting, deleting and rotating pages (cho phép chèn, xóa và quay trang).
- Các mục khác bạn để mặc định, sau đó nhấp **OK** để áp dụng (xem hình 3.63).

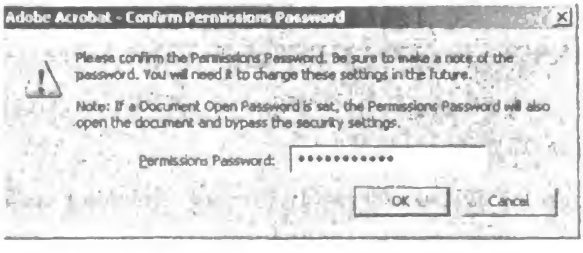
6. Trong hộp thoại Confirm Document Password, bạn nhập lại password mà bạn đã nhập trong mục Require a password to open the document vào ô **Document Open to Password**, sau đó nhấp **OK** để áp dụng (xem hình 3.64).



Hình 3.63: *Thiết lập trong hộp thoại Password Security.*

Hình 3.64: *Nhập lại truy cập.*

7. Bạn nhập lại password mà bạn đã nhập ở **Permission** password vào mục **Permission password** trong hộp thoại Confirm permission password, sau đó nhấp **OK** để áp dụng (xem hình 3.65).



Hình 3.65: *Nhập lại password ủy quyền.*

8. Lưu lại tài liệu.

Như vậy đến đây ta đã hoàn thành việc đặt password cho các tập tin có định dạng .pdf. Mỗi lần truy cập vào tập tin này, bạn phải nhập vào password mà bạn vừa đặt.

Chương 4:
PHỤC HỒI DỮ LIỆU ĐÃ MẤT

- **Tìm hiểu về quá trình lưu trữ.**
- **Ontrack Easy Data Recovery Professional.**
- **Chương trình Get Data Back for NTFS.**
- **Get Data Back for FAT.**
- **Data Doctor Recovery - NTFS-FAT.**
- **PhotoRescue Professional.**
- **Một số chương trình phục hồi dữ liệu khác.**

Công nghệ lưu trữ phát triển đã làm cho việc quản lý hồ sơ và bảo lưu tài liệu dễ dàng hơn. Ta không còn phải mất cả ngày thậm chí cả tuần để tìm kiếm dữ liệu trong những kho lưu trữ lớn. Tất cả dữ liệu được lưu trong máy tính, chỉ cần một vài thao tác là thông tin có thể hiển thị ngay trên màn hình.

Tuy nhiên, lưu trữ tài liệu trên máy tính cũng thường xuyên gặp các rủi ro như: Đĩa cứng bị hư hỏng ở một sector nào đó, tập tin, phần mềm bị lỗi, hoặc bạn vô tình xóa mất tập tin hay thư mục nào đó trong lúc vội vàng, mệt mỏi. Ngoài ra thông tin còn bị mất do các yếu tố phá hoại như: Virus, Trojan hay một hình thức phá hoại nào đó do đối thủ cạnh tranh gây ra. Chính vì thế dữ liệu quý giá của bạn đang đứng trước nguy cơ biến mất vĩnh viễn.

Chương này giới thiệu đến bạn một số giải pháp khôi phục dữ liệu một cách nhanh chóng, chính xác và toàn diện.

I. Tìm hiểu về quá trình lưu trữ

Thông tin được lưu trữ trên thiết bị được gọi chung là Media. Đĩa cứng cũng là một trong những thiết bị đó. Đĩa cứng gồm nhiều lá từ mỏng, trên mỗi lá từ này được chia làm các mặt gọi là Side (một lá từ có 2 side: side 0, side 1), mỗi một Side được chia thành nhiều vòng tròn đồng tâm, các vòng tròn đồng tâm này gọi là Track, mỗi Track chia

thành nhiều cung, mỗi cung được gọi là Sector, trong MS DOS, mỗi Sector có 512 bytes. Tập hợp nhiều Sector được gọi là Cluster. Số lượng sector trên một cluster là khác nhau ở các hệ điều hành khác nhau.

Thông tin được tổ chức và lưu trữ trên từng sector của đĩa cứng vật lý gọi là địa chỉ lưu trữ, mỗi một tập tin khi được lưu trữ trên đĩa đều có một địa chỉ nhất định và các địa chỉ này được quản lý bởi một danh mục, danh mục này được quy định bởi bảng tham số đĩa.

Chính vì vậy mà mỗi khi xóa một tập tin nào đó, ngay cả khi ta xóa sạch nó trong thùng rác của hệ điều hành thì hệ điều hành chỉ làm một nhiệm vụ đơn giản là xóa tên nó trong danh mục quản lý của bảng tham số đĩa. Nói một cách cụ thể đó là hệ điều hành chỉ xóa liên kết từ danh mục quản lý tập tin tới địa chỉ lưu trữ nó. Vì thế dữ liệu trên đĩa cứng tại những địa chỉ đó vẫn còn nguyên cho đến khi nó được ghi đè lên bởi một thông tin khác.

Lợi dụng điểm này, các công ty lập trình đã tạo ra các phần mềm để phục hồi lại những tập tin này, thực chất của việc phục hồi dữ liệu là tạo liên kết từ danh mục quản lý đến địa chỉ lưu trữ.

II. Ontrack Easy Data Recovery Professional

Đây là chương trình phục hồi dữ liệu chuyên nghiệp, nó giúp tìm lại được hầu hết các loại dữ liệu bị mất do các nguyên nhân: fdisk, format, xóa, hay do những chương trình phá hoại gây ra như virus hoặc bất kỳ một nguyên nhân nào khác dẫn đến dữ liệu bị mất.

Chương trình không cần cài đặt, bạn có thể sử dụng chương trình này ở thư mục Chapter 4. Sau khi giải nén, bạn vào thư mục chứa chương trình và chạy tập tin EasyRecovery.exe để mở chương trình.

1. Chẩn đoán dữ liệu trên đĩa

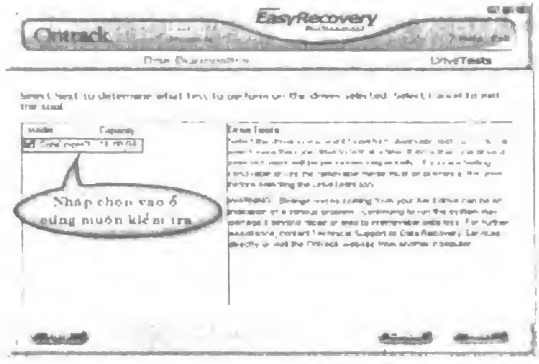
Mục này cho phép bạn kiểm tra toàn diện những thông tin trên đĩa cứng như: DriveTests, SmartTests, SizeManager, JumperViewer, PartitionTests, DataAdvisor.

1.1. Drive Tests

Chức năng này cho phép kiểm tra những lỗi tiềm tàng trên đĩa cứng của máy tính, từ đó bạn có thể khắc phục được những lỗi tìm được thông qua những chương trình chuyên dụng khác. Để kiểm tra đĩa cứng, bạn thực hiện như sau:

1. Tại giao diện chính của chương trình, chọn **Disk Diagnostics > TestDrives**.

2. Chương trình hiển thị danh sách các ổ đĩa trong máy tính, đánh dấu chọn vào ổ đĩa muốn kiểm tra, sau đó nhấp **Next** để tiếp tục (xem hình 4.1).

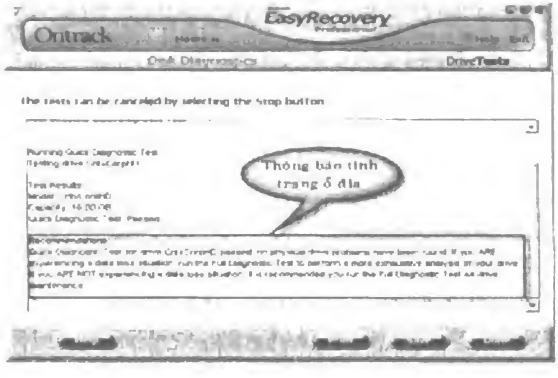


Hình 4.1: *Chọn ổ cứng muốn kiểm tra.*

3. Chương trình có hai mức kiểm tra, nhấp chọn vào mức mà bạn muốn kiểm tra, sau đó nhấp **Next** để tiếp tục.

- **Quick Diagnostics Test:** kiểm tra nhanh.
- **Full Diagnostics Test:** kiểm tra toàn diện, chương trình kiểm tra trên từng sector của đĩa và hiển thị các vấn đề theo danh sách.

4. Sau khi quá trình kiểm tra kết thúc, chương trình hiển thị tình trạng ổ đĩa mà chương trình phân tích được trên giao diện chính. Khi chương trình hiển thị nút **Done** thì lúc này quá trình kiểm tra đã kết thúc (xem hình 4.2).



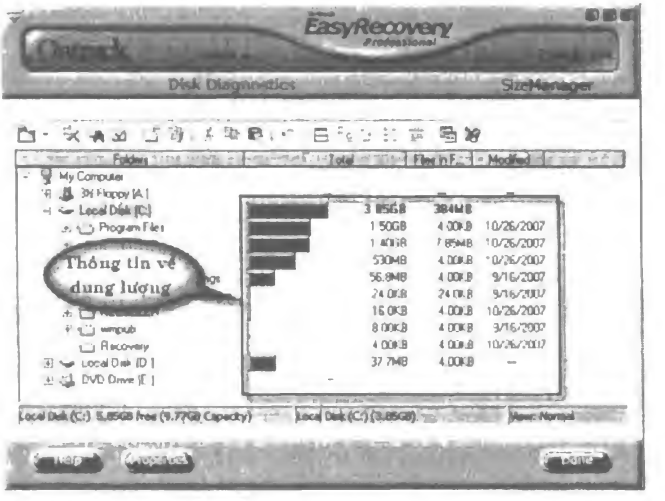
Hình 4.2: *Thông báo tình trạng ổ đĩa.*

1.2. Size Manager

Đây là chức năng cho phép kiểm tra dung lượng và các thư mục trên đĩa cứng. Kết quả thống kê được hiển thị thành những lưu đồ hình cột để biểu thị dung lượng của các mục. Phương pháp thực hiện bạn làm như sau:

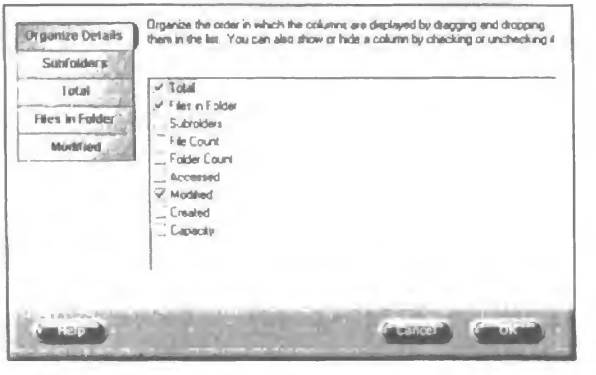
1. Chọn **Disk Diagnostics > Size Manager**.

Chương trình sẽ thống kê danh sách các ổ đĩa trong máy tính, bạn nhấp chọn vào ổ đĩa muốn kiểm tra, sau đó nhấp **Next** để thực hiện (xem hình 4.3).



Hình 4.3: *Thông tin về dung lượng.*

2. Nếu muốn theo dõi thông tin chi tiết của một phân vùng nào đó hoặc thư mục nào đó, bạn nhấp chọn vào đối tượng muốn xem, sau đó nhấp **Properties** để thực hiện (xem hình 4.4).



Hình 4.4: *Thông tin chi tiết của ổ đĩa hoặc thư mục.*

Nếu không muốn thực hiện nữa, bạn nhấp nút **Cancel** để quay về giao diện chính của chương trình.

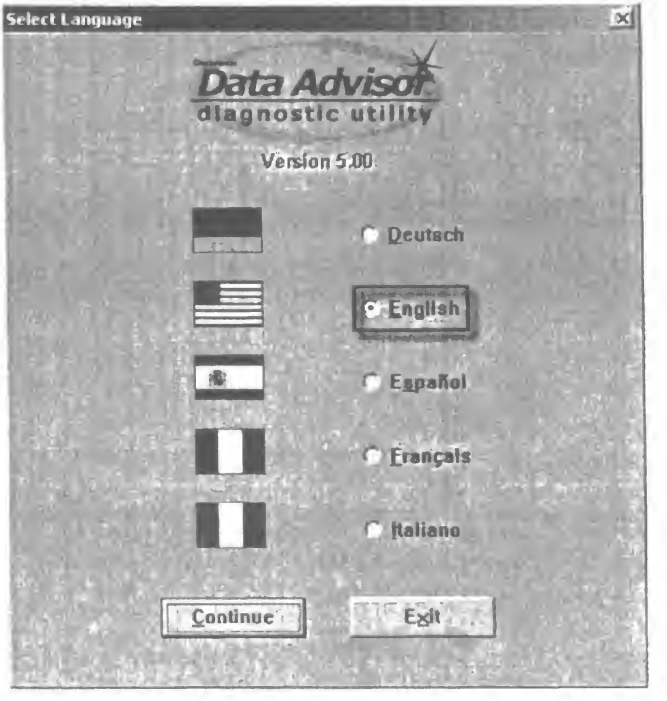
1.3. Data Advisor

Vì đây là chương trình hỗ trợ việc tìm kiếm và phục hồi dữ liệu trên cả 2 môi trường Windows và MS DOS, nên nó cũng hỗ trợ tiện ích tạo ổ đĩa boot (đĩa khởi động). Thực hiện theo các bước sau:

1. Chọn **Disk Diagnostics > DataAdvisor**.

   Đây là tiện ích giúp tạo ổ đĩa mềm (floppy) khởi động.

2. Tiếp theo, bạn chọn ngôn ngữ gán cho chương trình trong đĩa mềm, ví dụ **English**, sau đó nhấp **Continue** để tiếp tục (xem hình 4.5).



Hình 4.5: *Chọn ngôn ngữ gán cho chương trình.*

3. Chương trình thông báo tình trạng bản quyền của chương trình, bạn nhấp nút **Continue** để tiếp tục.

4. Tiếp theo chương trình sẽ đưa ra luật bản quyền, nếu bạn đồng ý với những mục mà chương trình đưa ra thì nhấp nút **Yes** để tiếp tục (xem hình 4.6).

Hình 4.6: *Luật bản quyền mà chương trình thông báo.*

5. Chương trình sẽ thông báo tất cả dữ liệu đĩa mềm của bạn sẽ bị mất hết để ghi những tập tin cần thiết cho việc khởi động máy tính. Tiếp theo chương trình cũng yêu cầu bạn chèn đĩa mềm vào ổ đĩa, bạn thực hiện theo yêu cầu và nhấp nút **Start** để bắt đầu (xem hình 4.7).

Hình 4.7: *Tiến hành quá trình tạo đĩa mềm Boot.*

2. Phục hồi dữ liệu đã mất

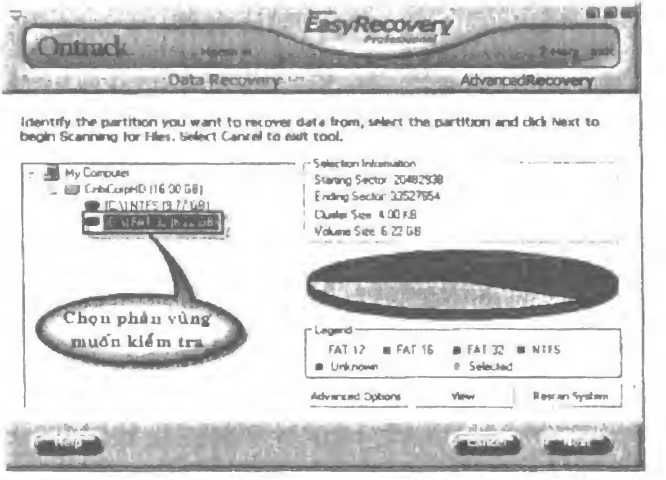
Mục này cho phép bạn phục hồi lại những liệu đã mất do các nguyên nhân như: Những tập tin đã bị xóa hoặc bị hư hại do các chương trình phá hoại như virus, format hay fdisk...

2.1. Advanced Recovery

Trong mục này cho phép sử dụng những thiết lập nâng cao để tìm lại những tập tin hoặc thư mục, để thực hiện bạn làm như sau:

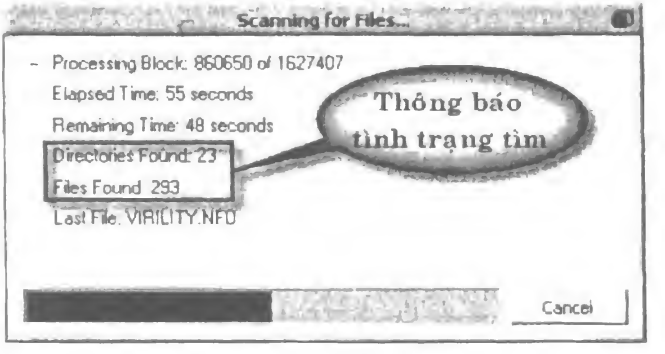
1. Chọn **Data Recovery > Advanced Recovery**.

Chọn phân vùng muốn phục hồi, sau đó nhấp **Next** để tiếp tục (xem hình 4.8).



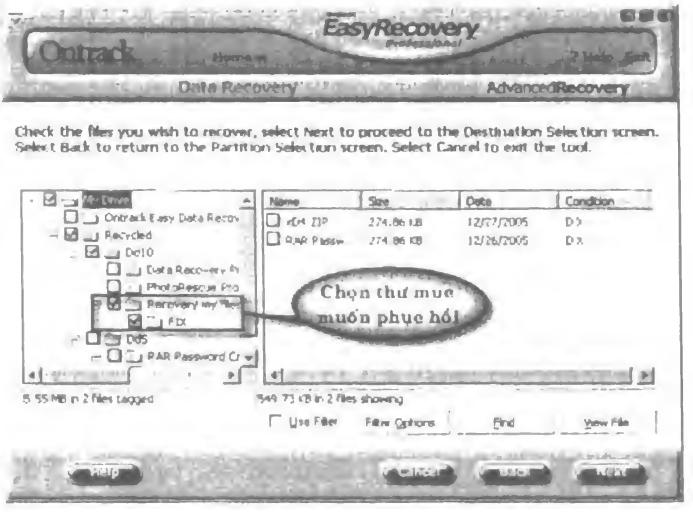
Hình 4.8: *Chọn phân vùng muốn phục hồi.*

2. Chương trình sẽ tiến hành tìm kiếm trên từng sector và thông báo tình trạng tìm kiếm hiện thời (xem hình 4.9).



Hình 4.9: *Tình trạng tìm kiếm hiện thời.*

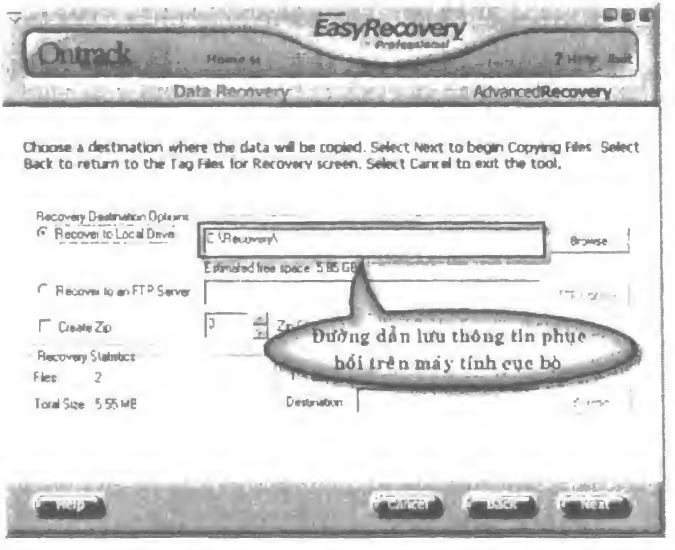
3. Sau khi quá trình tìm kiếm kết thúc, chương trình sẽ hiển thị danh sách các tập tin và thư mục tìm được. Nhấp chọn vào các tập tin và thư mục muốn phục hồi, sau đó nhấp **Next** để tiếp tục (xem hình 4.10).



Hình 4.10: *Chọn thư mục hay tập tin muốn phục hồi.*

4. Nhấp chọn vào mục **Recovery to Local Drive**, sau đó nhấp nút **Browse** để chọn đích lưu thông tin muốn phục hồi, sau đó nhấp **Next** để thực hiện.

Mục này cho phép bạn lưu những thông tin phục hồi trên đĩa cứng của máy tính cục bộ (xem hình 4.11).



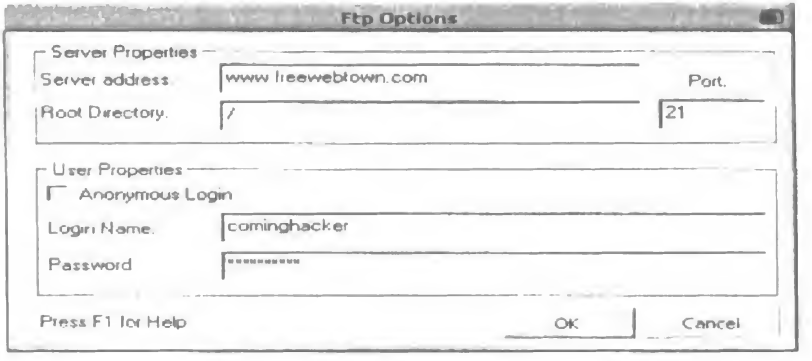
Hình 4.11: *Lưu thông tin phục hồi trên máy tính cục bộ.*

Như vậy đến đây ta đã hoàn thành việc lưu thông tin muốn phục hồi lên thư mục Recovery trên ổ đĩa C của máy tính.

5. Nhấp chọn vào **Recovery to an FTP Server**, tiếp theo nhấp chọn vào mục **Create Zip**, sau đó nhấp nút **FTP Options** và thiết lập như các mục sau:

- **Server Address:** địa chỉ webserver, ví dụ www.freewebtown.com.
- **Root Directory:** thư mục gốc trên FTP Server: ví dụ /
- **Login name:** tên tài khoản trên Webserver, ví dụ cominghacker.
- **Password:** nhập vào password của tài khoản mà bạn đã đăng ký.
- **Port:** cổng mặc định của FTP Server là 21.

Tiếp theo, nhấp **OK** để áp dụng (xem hình 4.12).



Hình 4.12: *Lưu thông tin phục hồi vào FTP Server.*

Hướng dẫn thêm:

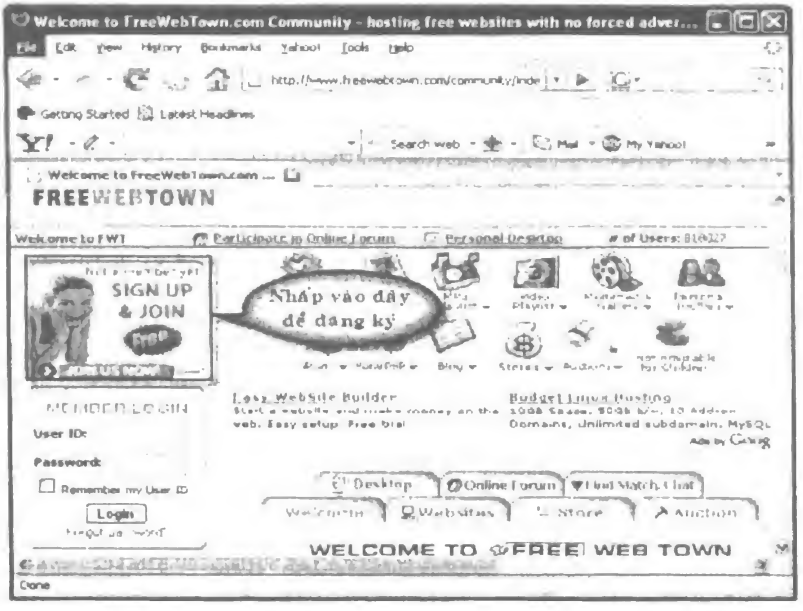
Để sử dụng được bước 5 thì trước tiên bạn phải tạo cho mình một tài khoản trên FTP Server, dưới đây chúng tôi sẽ hướng dẫn bạn tạo một tài khoản FTP Server trên trang www.freewebtown.com.

1. Tạo tài khoản trên www.freewebtown.com

Trang này cho phép bạn tạo một hoặc nhiều tài khoản và không cần kích hoạt, hơn nữa băng thông cũng tương đối lớn và dung lượng lưu trữ 1 GB, không giới hạn kích thước tập tin upload, hỗ trợ FTP client... Để tạo tài khoản, bạn thực hiện các bước sau:

1. Mở Internet Explorer hoặc Mozilla Firefox hay bất kỳ một trình duyệt nào. Trên thanh Address của các trình duyệt, bạn nhập www.freewebtown.com, tiếp theo nhấn **Enter** để thực hiện.

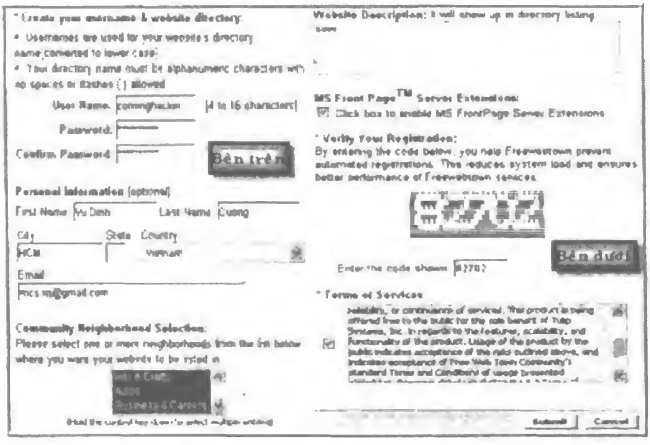
2. Nhấp nút **Sign Up & Join** để tạo tài khoản và đăng nhập (xem hình 4.13).



Hình 4.13: *Giao diện của Freewebtown.*

3. Tiếp theo, bạn nhập các thông tin sau:

- **User name:** tên tài khoản đăng nhập, ví dụ cominghacker.
- **Password:** nhập vào password cho tài khoản.
- **Confirm password:** nhập lại password.
- **First name:** họ và tên lót của bạn, ví dụ Vu Dinh.
- **Last name:** tên của bạn, ví dụ Cuong.
- **City:** nhập tên thành phố, ví dụ HCM.
- **Country:** chọn VietNam.
- **Email:** nhập vào địa chỉ email của bạn, ví dụ vncs.vn@gmail.com.
- **Web Description:** nhập thông tin mô tả, ví dụ Save.
- **MS Front Page™ Server Extensions:** nhấp chọn vào mục bên dưới, nếu bạn muốn sử dụng FontPage để soạn Web.
- **Enter the code shown:** nhập những ký tự mà trong mục hiển thị. Ví dụ 82702, số này là số ngẫu nhiên, được tạo ngẫu nhiên mỗi khi bạn tạo một tài khoản mới, tiếp theo nhấp nút **Submit** để hoàn thành (xem hình 4.14).



Hình 4.14: *Những thông tin đăng ký.*

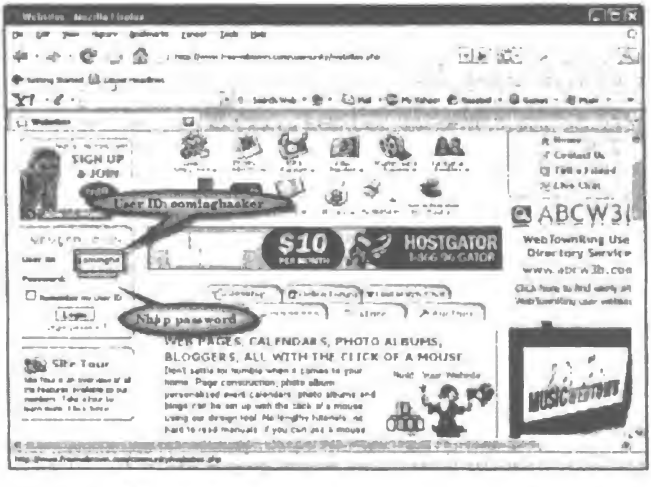
Như vậy, đến đây ta đã hoàn thành việc đăng ký tài khoản trên **www.freewebtown.com**, việc tiếp theo là đăng nhập và sử dụng.

2. Đăng nhập trực tiếp từ web site

Bạn có thể upload dữ liệu trực tiếp từ trình duyệt thông qua website, để sử dụng tiện ích này bạn thực hiện các bước sau:

1. Mở trình duyệt Mozilla Firefox hoặc Internet Explorer, sau đó trong thanh Address nhập **www.freewebtown.com**.

2. Tại mục **User ID**, bạn nhập **cominghacker**, mục **Password**, nhập vào password cho tài khoản này. Tiếp theo nhấp nút **Login** (xem hình 4.15).

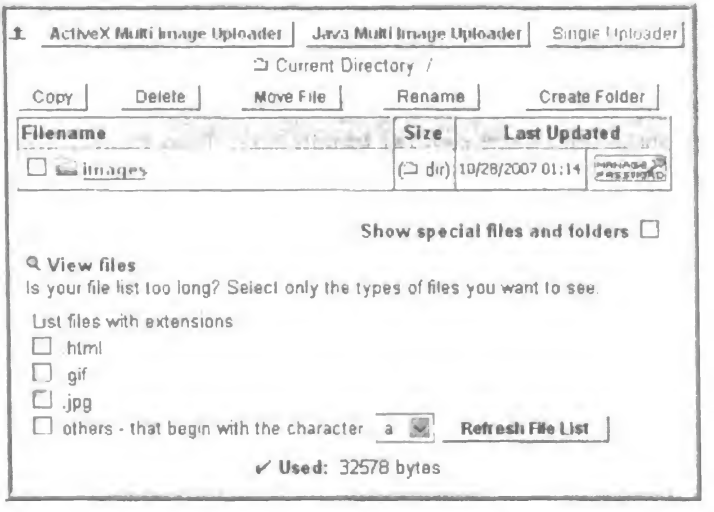


Hình 4.15: *Nhập user ID và password đăng nhập.*

3. Kéo thanh trượt xuống và nhấp nút **File Manager** để mở cửa sổ quản lý tập tin (xem hình 4.16).

Hình 4.16: *Mở cửa sổ quản lý file.*

4. Tại cửa sổ quản lý tập tin này, bạn có thể thêm, xóa, sửa và soạn thảo các tập tin (xem hình 4.17).



Hình 4.17: *Những tiện ích trong cửa sổ File manager.*

3. Đăng nhập bằng WS_FTP Pro

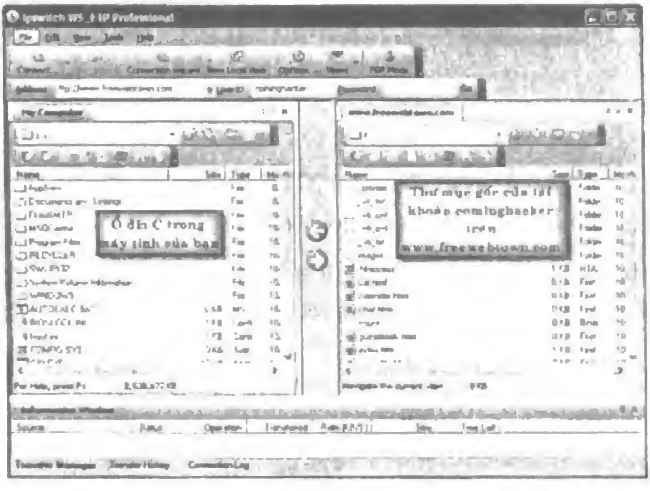
Đây là chương trình FTP client cho phép máy tính của bạn kết nối với Web server để download, upload dữ liệu theo giao thức truyền file FTP.

Chương trình được cung cấp trong thư mục Genaral Software, bạn có thể download tại website www.minhkhai.com.vn. Sau khi giải nén và cài đặt, bạn thực hiện như sau:

1. Vào **Start > Programs > Ipswitch WS_FTP Pro > WS_FTP Pro** để mở chương trình.
2. Tại giao diện chính của chương trình, bạn nhập các thông tin sau:

- **Address:** ftp://www.freewebtown.com
- **User ID:** cominghacker.
- **Password:** Nhập vào password mà bạn đã đăng ký cho tài khoản cominghacker.

Tiếp theo, nhấn **Enter** để đăng nhập (xem hình 4.18).



Hình 4.18: *Đăng nhập vào web server bằng WS_FTP Pro.*

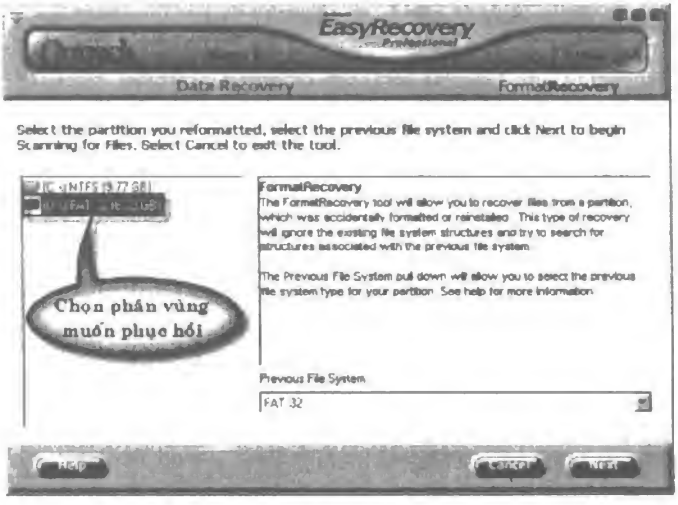
3. Sau khi đăng nhập thành công như hình 4.18, bạn có thể thao tác giữa máy tính của bạn và remote host, như là thao tác trên máy tính cục bộ. Điều này có nghĩa là, bạn có thể thêm, xóa, sửa, copy, cut, paste, rename..., ở remote host và máy tính cục bộ như thao tác giữa các mục trên máy tính cá nhân.

Như vậy, đến đây ta đã tạo, truy cập và quản lý một host một cách thành công. Từ nay, bạn có thể sử dụng host này để lưu trữ trực tuyến dữ liệu và có thể chia sẻ tài liệu cho bất kỳ ai.

2.2. Format Recovery

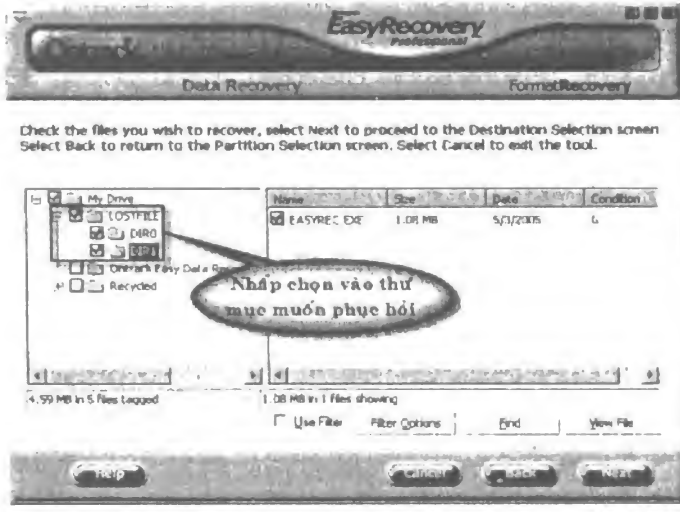
Mục này cho phép tìm lại những tập tin trong những phân vùng mà bạn vô tình format, phương pháp thực hiện như sau:

1. Chọn **Data Recovery > Format Recovery**, chương trình sẽ hiển thị danh sách các ổ đĩa và các phân vùng của các ổ đĩa vật lý hiện có trong máy tính, bạn nhấp vào phân vùng muốn phục hồi, sau đó nhấp **Next** để tiếp tục (xem hình 4.19).



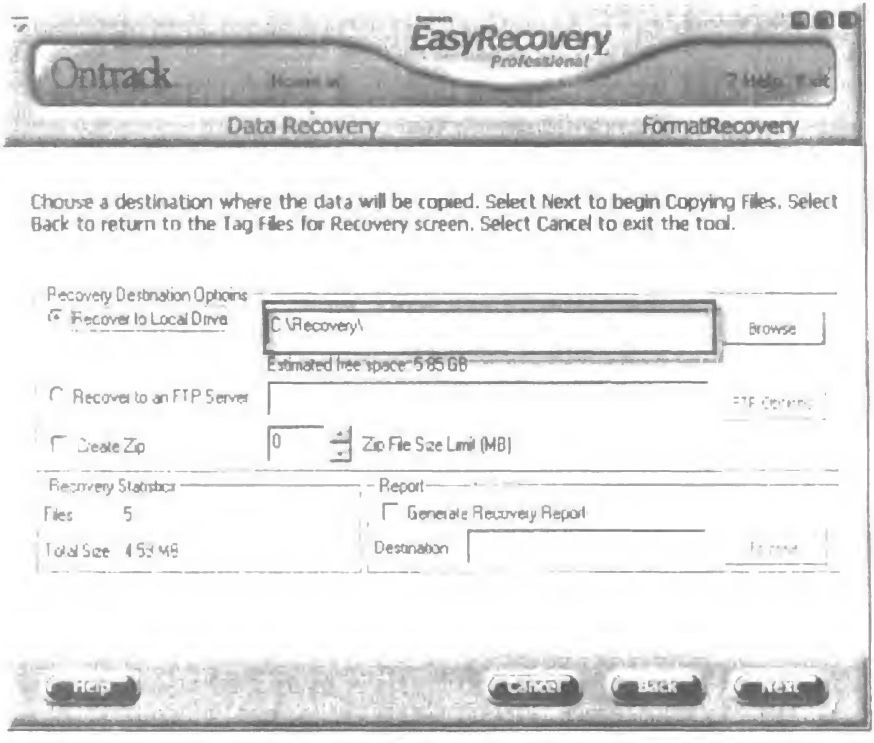
Hình 4.19: *Chọn phân vùng muốn phục hồi.*

2. Đợi chương trình quét trên bề mặt của đĩa cứng để tìm những tập tin, thư mục do format mà mất. Sau đó chương trình sẽ thống kê những thông tin tìm được dưới dạng cây thư mục. Bạn nhấp chọn vào thư mục muốn phục hồi sau đó nhấp **Next** để tiếp tục (xem hình 4.20).



Hình 4.20: *Chọn thư mục muốn phục hồi.*

3. Nhấp chọn vào mục **Recovery to Local Drive**, sau đó nhấp nút **Browse** để chọn đường dẫn lưu thư mục muốn phục hồi, ví dụ lưu ở **C:\Recovery** (xem hình 4.21).



Hình 4.21: *Chọn đường dẫn lưu thư mục phục hồi*

Như vậy, đến đây ta đã hoàn thành việc phục hồi những tập tin, thư mục do format mà mất.

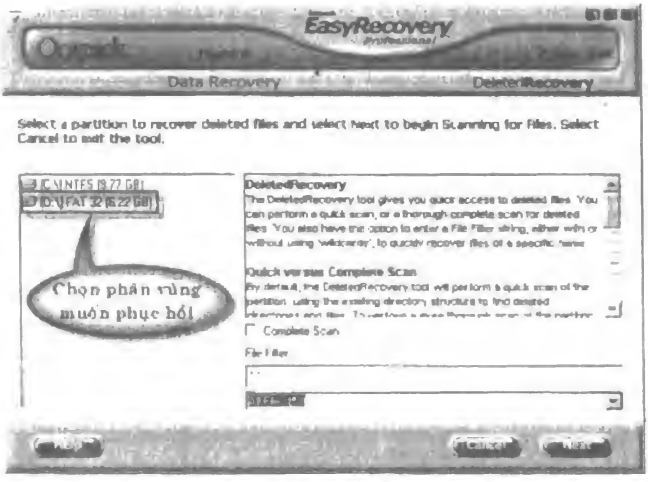
2.3. Deleted Recovery

Mục này cho phép bạn tìm lại những tập tin, thư mục do bạn đã xóa, hoặc những chương trình phá hoại gây ra, phương pháp thực hiện như sau:

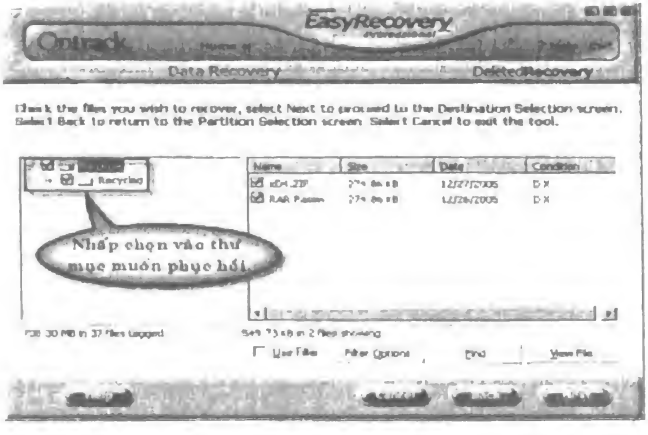
1. Chọn **Data Recovery > Deleted Recovery**.

Chương trình sẽ hiển thị danh sách các ổ đĩa vật lý và các phân vùng của ổ đĩa này trong giao diện của nó, bạn chọn phân vùng muốn phục hồi, sau đó nhấp **Next** để tiếp tục (xem hình 4.22).

2. Chương trình sẽ hiển thị những gì tìm thấy trong **Recycled**, bạn nhấp chọn vào thư mục muốn phục hồi, sau đó nhấp **Next** để tiếp tục (xem hình 4.23).



Hình 4.22: *Chọn phân vùng muốn phục hồi.*



Hình 4.23: *Chọn thư mục phục hồi.*

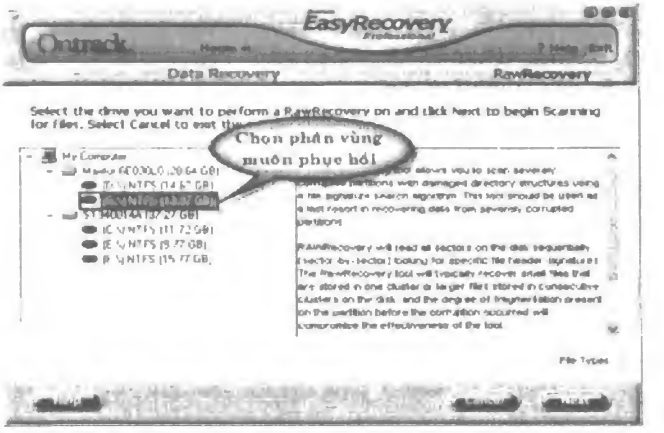
3. Tiếp theo, bạn chọn đường dẫn lưu thư mục như trong bước 3 của mục "**Format Recovery**".

2.4. Raw Recovery

Đây là công cụ cho phép bạn quét những phân vùng bị hư hại trên đĩa cứng của bạn và những cấu trúc thư mục bị hư hại nặng. nó sử dụng giải thuật tìm kiếm tín hiệu tập tin. Công cụ này cũng cho phép bạn sắp xếp lại những dữ liệu tìm được từ những phân vùng bị hư hại. Phương pháp thực hiện như sau:

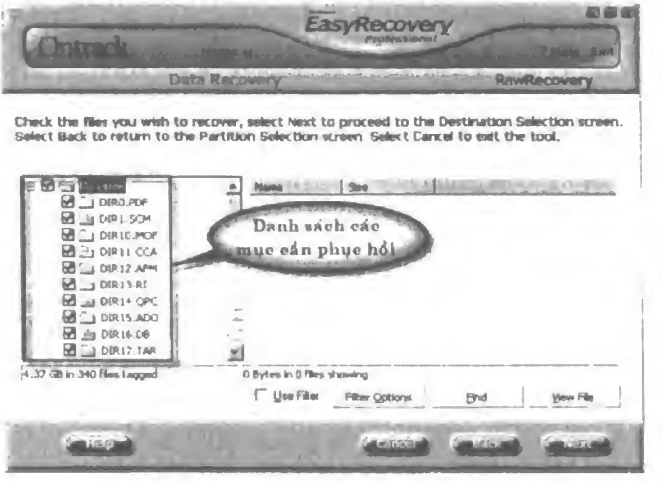
1. Vào **Data Recovery > Raw Recovery**.

Chương trình sẽ liệt kê danh sách các ổ đĩa vật lý và các phân vùng của các ổ đĩa này, tiếp theo nhấp chọn vào phân vùng muốn phục hồi, sau đó nhấp **Next** để tiếp tục (xem hình 4.24).



Hình 4.24: *Chọn phân vùng muốn phục hồi.*

2. Nhấp chọn vào danh sách các mục muốn phục hồi sau đó nhấp **Next** để tiếp tục (xem hình 4.25).



Hình 4.25: *Chọn danh sách các mục cần phục hồi.*

3. Chọn đường dẫn lưu thông tin phục hồi như ở bước 3 của mục "**Deleted Recovery**".

Như vậy tới đây ta đã hoàn thành quá trình tìm thông tin bị mất trên đĩa cứng. Ngoài ra, trong mục Data Recovery còn rất nhiều tiện ích khác phục vụ cho việc phục hồi thông tin bị mất. Bạn có thể khám phá thêm khi sử dụng chương trình.

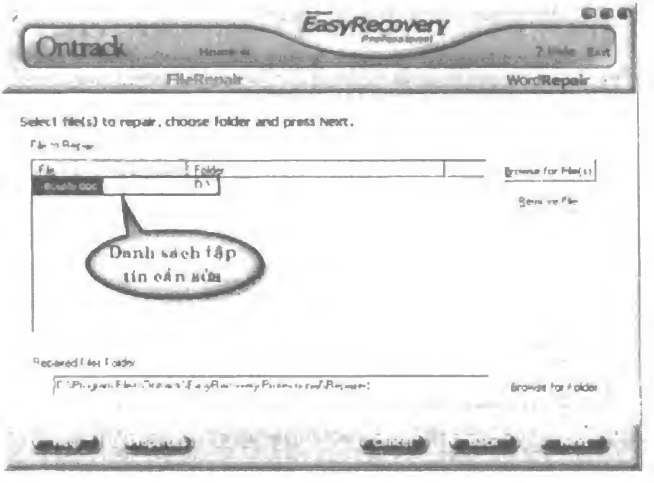
3. File Repair

Khi phục hồi lại dữ liệu sẽ không tránh khỏi tình trạng một số tập tin bị hư hại, vì thông tin trong những tập tin đó có thể đã bị chuyển đổi sai lệch, vì vậy mà dẫn đến tình trạng không thể xem được toàn vẹn thông tin. Có những chương trình hỗ trợ phương pháp sửa chữa một số loại tập tin như: MS Word, Excel, PowerPoint, Access và Winzip. Mục dưới đây sẽ giới thiệu một số chương trình đó.

3.1. Word Repair

Chương trình này cho phép sửa chữa những tập tin có định dạng .doc của MS Word, phương pháp thực hiện như sau:

1. Vào **File Repair > Word Repair**.
2. Nhấp nút **Browse for Files** để mở những tập tin Word muốn sửa (xem hình 4.26).
3. Nhấp nút **Browse for Folder** để mở thư mục lưu trữ những tập tin sau khi sửa, sau đó nhấp **Next** để thực hiện.



Hình 4.26: *Danh sách các tập tin cần sửa.*

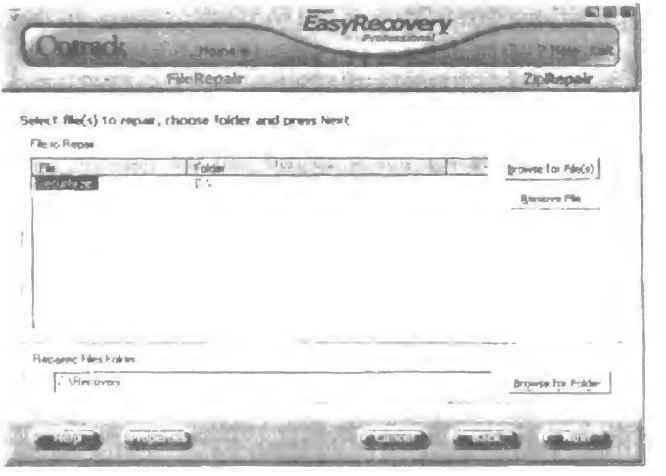
3.2. Zip Repair

Những tập tin có định dạng .zip là những tập tin hay bị lỗi nhất, nhất là trong trường hợp tập tin được phục hồi lại. Để khắc phục tình trạng này, chương trình cho chúng ta giải pháp Repair lại những tập tin ZIP bị lỗi, phương pháp thực hiện như sau:

1. Chọn **File Repair > Zip Repair**.

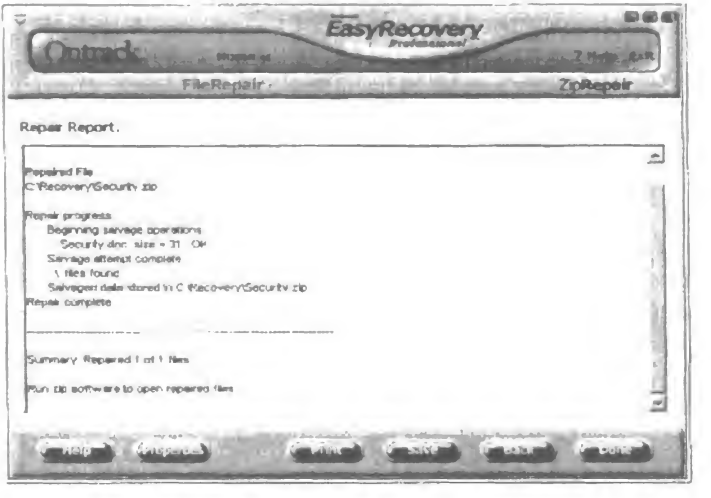
2. Nhấp nút **Browse for Files** để mở những tập tin có định dạng .zip muốn sửa.

3. Nhấp nút **Browse for Folder** để lưu những tập tin mà chương trình sửa được (xem hình 4.27).



Hình 4.27: *Chọn tập tin muốn sửa và đường dẫn lưu file.*

4. Chương trình sẽ hiển thị những thông tin về tập tin mà nó sửa, thông tin bao gồm, dung lượng, và tình trang sửa chữa (xem hình 4.28).



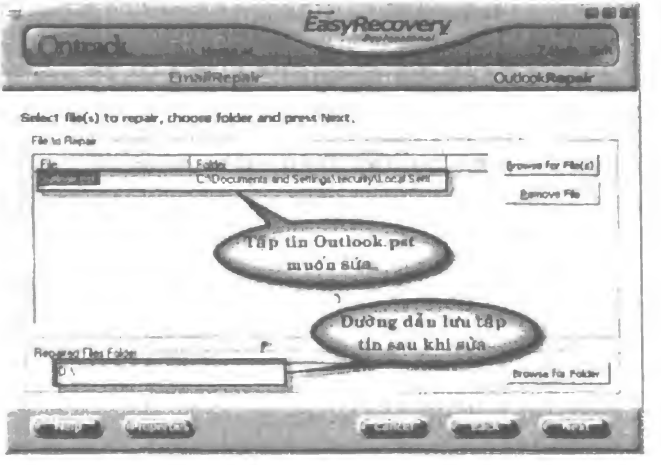
Hình 4.28: *Những thông tin sau khi sửa.*

Bạn áp dụng cách tương tự để sửa chữa những tập tin của Access, PowerPoint, Excel.

4. Email Repair

Mục này cho phép bạn sửa chữa những tập tin có định dạng **.pst** của MS Outlook, đây là những tập tin lưu trữ nội dung của email. Những tập tin này thường được lưu trữ tại C:\Documents and Settings\security\Local Settings\Application Data\Microsoft\Outlook, trong đó **Security** là tài khoản mà bạn đăng nhập vào máy tính.

1. Chọn **Email Repair > Outlook Repair**.
2. Nhấp nút Browse for Files để mở tập tin .pst muốn sửa. Ví dụ, sửa tập tin **outlook.pst** trong thư mục **C:\Documents and Settings\ security\Local Settings \Application Data\Microsoft\Outlook**.
3. Nhấp nút **Repair File Folder** để chọn thư mục lưu trữ tập tin .pst mà chương trình sửa được, sau đó nhấp **Next** để thực hiện (xem hình 4.29).



Hình 4.29: *Những thông tin sửa chữa.*

Trên đây là những thông tin cần thiết, những chức năng cơ bản nhất của chương trình. Ngoài ra, chương trình còn rất nhiều những tiện ích và công cụ khác, các bạn có thể khám phá thêm khi sử dụng chương trình.

III. Chương trình Get Data Back for NTFS

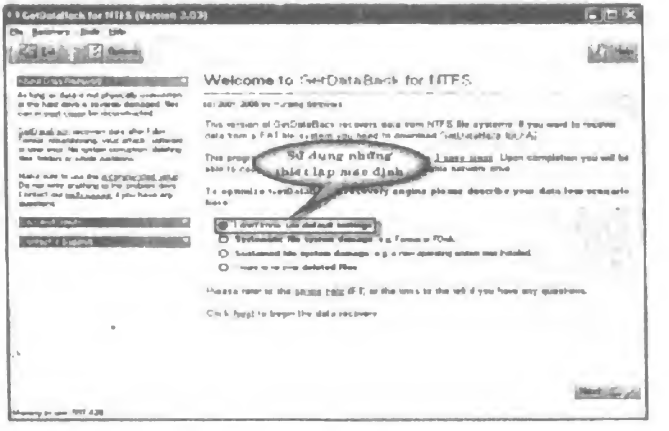
Chương trình cho phép tìm lại tất cả các dữ liệu bị mất do: fdisk, format, hay bị các chương trình phá hoại gây ra như: virus, worm, lỗi phần mềm hoặc những tập tin đã xóa trên những ổ đĩa có phân vùng được định dạng theo định dạng NTFS.

Chương trình này tương thích với Windows 2K/XP, bạn có thể download phần mềm này tại website www.minhkhai.com.vn, thư mục Chapter 4. Sau khi giải nén và cài đặt chương trình, bạn thực hiện như sau:

1. Sử dụng những thiết lập mặc định

Nếu bạn không muốn tự mình lựa chọn những thiết lập phức tạp để khôi phục dữ liệu thì phương pháp này sẽ giúp bạn nhanh chóng thực hiện.

1. Trên giao diện chính của chương trình, nhấp chọn vào mục **I don't know, use default settings**, sau đó nhấp **Next** để tiếp tục (xem hình 4.30).



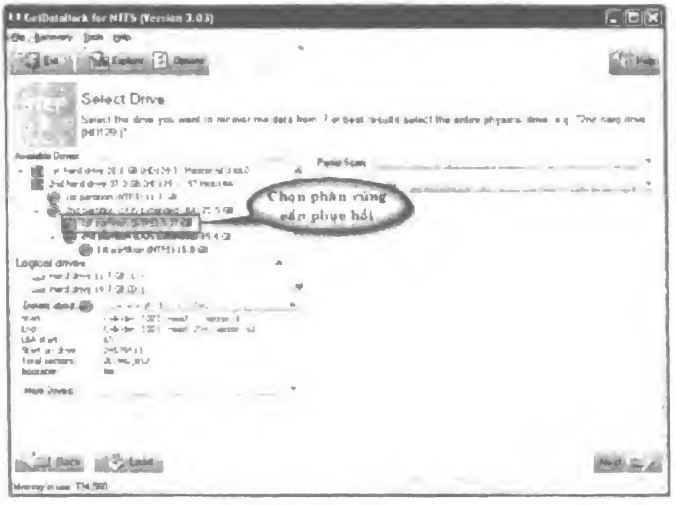
Hình 4.30: *Sử dụng những thiết lập mặc định.*

2 Chương trình sẽ thống kê trong máy tính có bao nhiêu đĩa cứng và hiển thị số phân vùng trên từng đĩa cứng này. Để phục hồi dữ liệu của phân vùng nào, bạn chỉ cần nhấp chọn phân vùng của ổ đĩa đó.

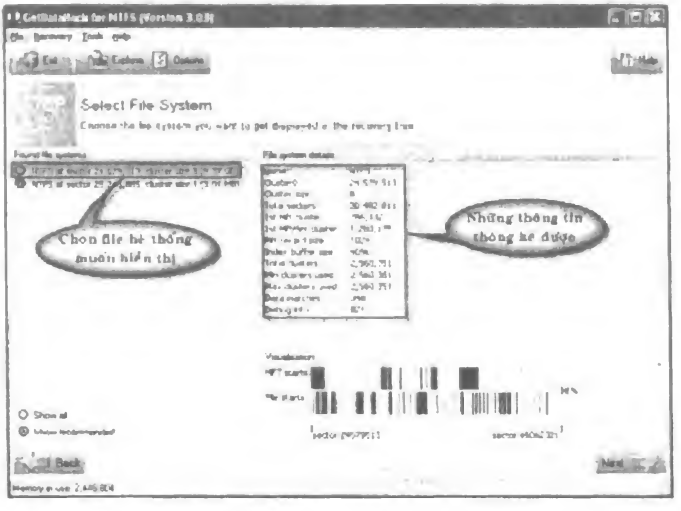
Ví dụ, phục hồi tất cả dữ liệu trong ổ đĩa **2nd hard drive** ở ổ đĩa E, tại mục Available Drives, chọn **2nd hard drives 37.3 GB (HD129:) – ST340014A > 1st partition NTFS 9.77 GB**, sau đó nhấp **Next** để tiếp tục (xem hình 4.31).

3. Nhấp vào tập tin hệ thống muốn hiển thị sau đó nhấp **Next** để tiếp tục.

Ví dụ, chọn **NTFS at sector 24,579,513, cluster size 8 (9.77)**, sau đó nhấp **Next** để tiếp tục (xem hình 4.32).



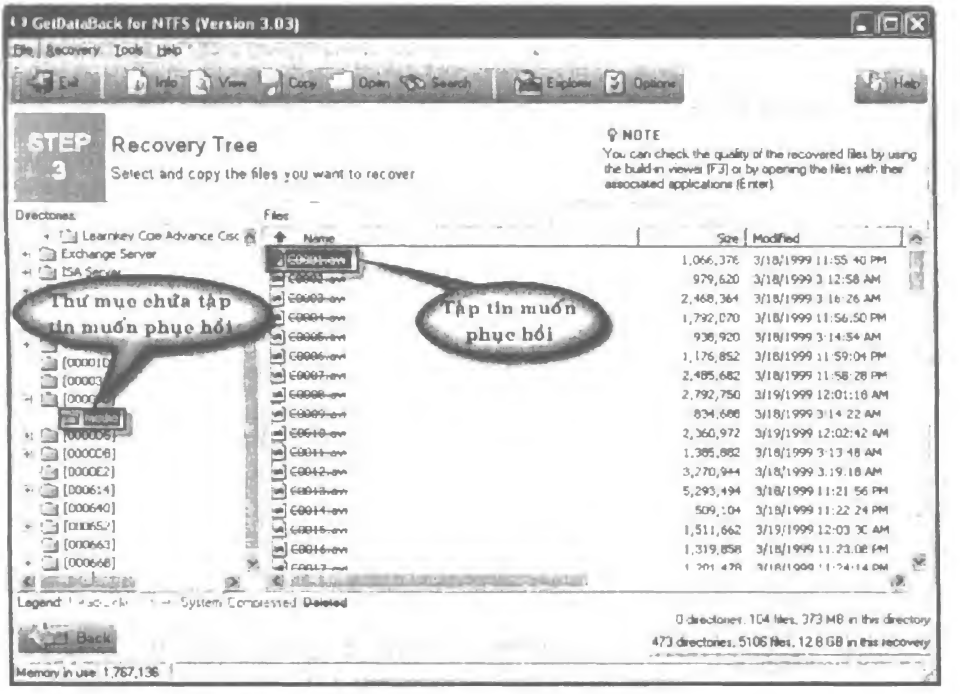
Hình 4.31: *Chọn phân vùng cần phục hồi.*



Hình 4.32: *Những thông tin thống kê được.*

4. Danh sách những tập tin mà chương trình tìm thấy được hiển thị ngay trên giao diện của chương trình. Để phục hồi tập tin nào bạn nhấp chọn vào tập tin đó, tiếp theo nhấn phím **F5** để copy, chương trình sẽ xuất hiện hộp thoại thông báo đường dẫn lưu tập tin phục hồi, tại hộp thoại này, chọn đường dẫn lưu tập tin, sau đó nhấp **OK** để áp dụng.

Ví dụ, phục hồi lại tập tin có tên **C001** trong thư mục Media, nhấp đôi vào thư mục **Media** và nhấp chọn vào tập tin **C001** (xem hình 4.33).



Hình 4.33: *Chọn thư mục hoặc tập tin muốn phục hồi.*

5. Nhấn phím **F5** trên bàn phím để mở hộp thoại Copy files, trong mục To, bạn nhấp nút **Browse for directory** để chỉ định thư mục lưu tập tin, thư mục mặc định là **C:\Documents and Settings\security**, tiếp theo nhấp **OK** để phục hồi.

Security là thư mục tương ứng với tên tài khoản đăng nhập vào máy tính (xem hình 4.34)

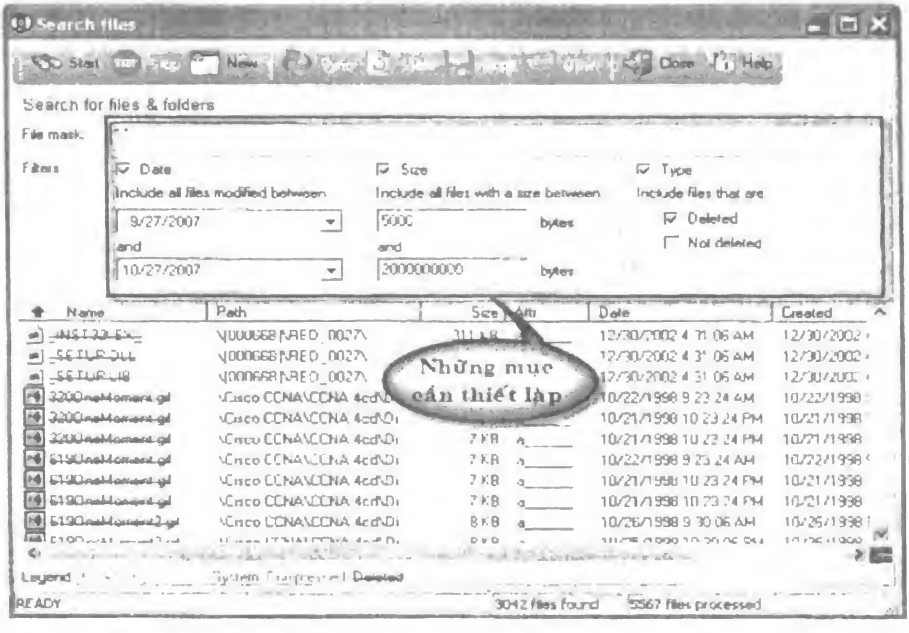
Hình 4.34: *Chỉ đường dẫn lưu tập tin.*

6. Nếu nhớ rõ tên tập tin muốn phục hồi thì ngay trên giao diện chính của chương trình, nhấp nút **Search** hoặc vào menu **Tools > Search files** để mở hộp thoại Search file.

Ví dụ, tìm tất cả những tập tin đã xóa vào khoảng giữa 27/09/2007 đến 27/10/2007 và những tập tin có kích thước giữa 5000 – 2000000000 bytes. Chỉ tìm những tập tin đã xóa, bạn thiết lập như sau:

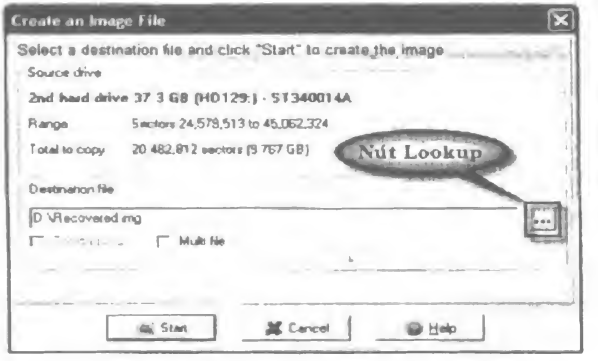
- **File mask:** *.* (tất cả các files).
- **Include all file modified between:** nhập 9/27/2007.
- **And:** nhập 10/27/2007.
- **Include all files with a size between:** nhập 5000.
- **And:** nhập 2000000000.
- **Include files that are:** nhấp chọn **Deleted**.

Tiếp theo, nhấp nút **Start** để thực hiện tìm (xem hình 4.35).



Hình 4.35: *Những thiết lập trong hộp thoại Search files.*

7. Để nhóm tất cả những thông tin tìm được vào một tập tin img. Vào menu **Tools > Create Image File** để mở hộp thoại Create an Image File, tiếp theo nhấp nút **Lookup** để đặt tên và chỉ định nơi lưu trữ tập tin (xem hình 4.36).

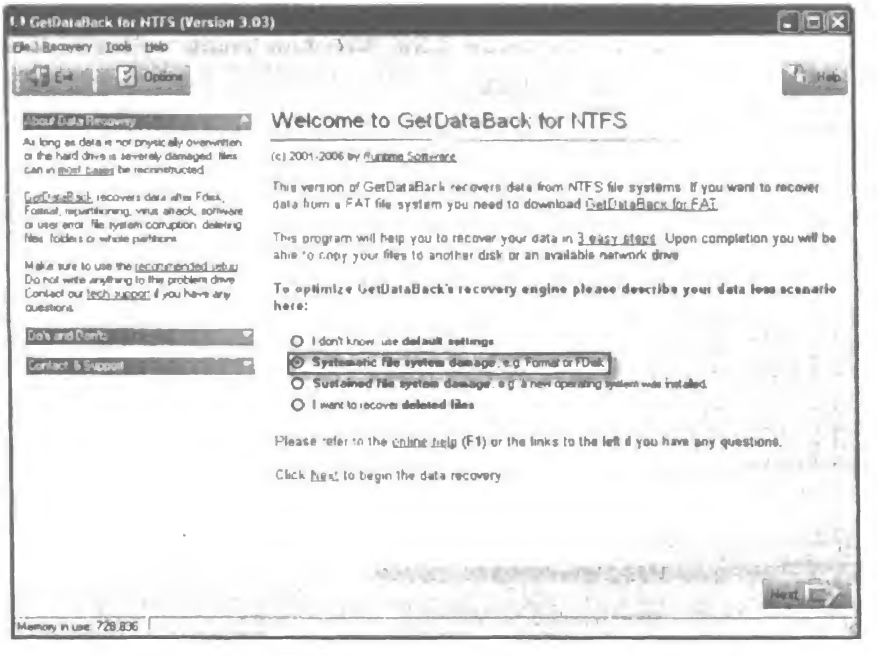


Hình 4.36: *Tạo file .img.*

2. Phục hồi thông tin bị mất do Fdisk hay Format

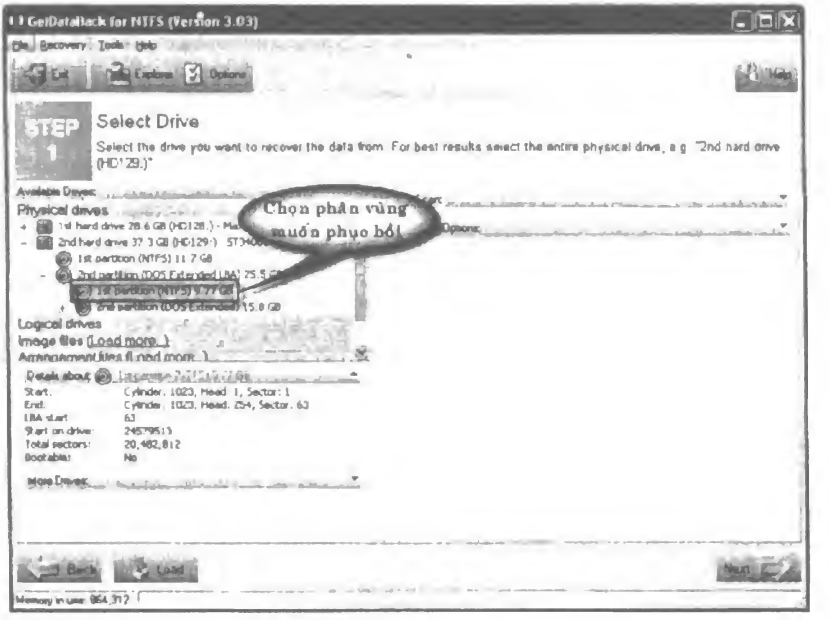
Đây là lựa chọn cho phép phục hồi những tập tin hệ thống bị mất do Fdisk hoặc Format, để thực hiện, bạn làm như sau:

1. Trên giao diện chính của chương trình, nhấp chọn vào mục **Systematic file system damage**, sau đó nhấp **Next** để tiếp tục (xem hình 4.37).



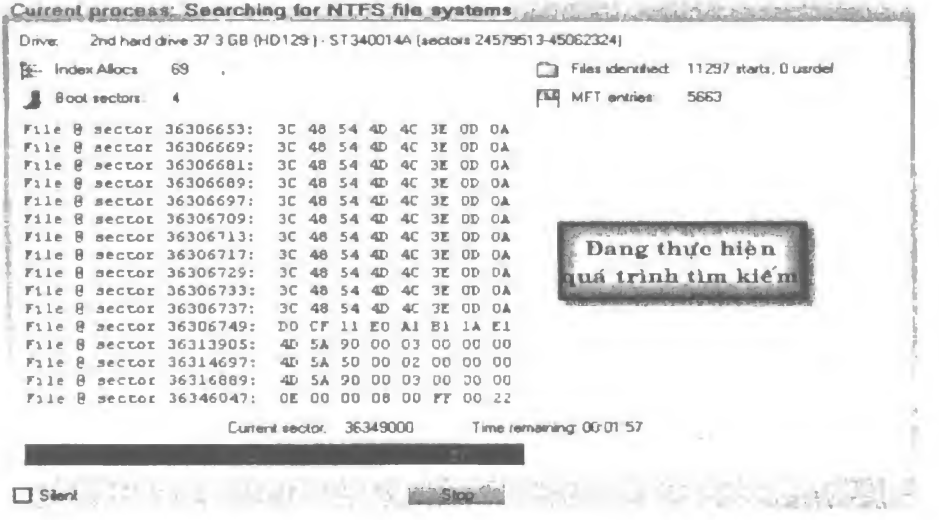
Hình 4.37: *Chọn Systematic file system damage.*

2. Nhấp chọn ổ đĩa và phân vùng muốn phục hồi, sau đó nhấp **Next** để tiếp tục (xem hình 4.38).



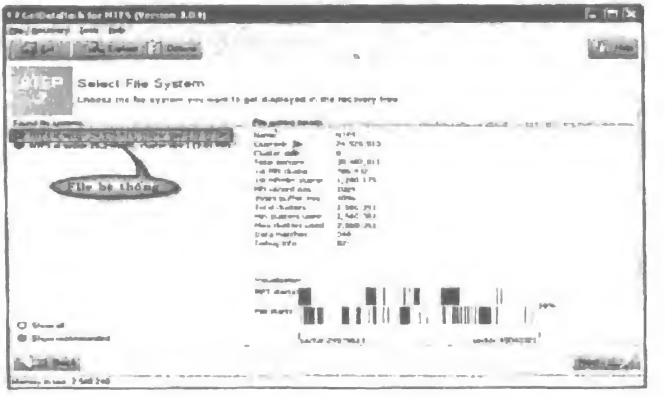
Hình 4.38: *Chọn phân vùng muốn phục hồi.*

Sau khi nhấp nút Next, chương trình bắt đầu tìm kiếm, những thông tin được hiển thị như hình 4.39. Nếu bạn muốn ngừng quá trình tìm kiếm, nhấp nút **Stop** để ngưng.



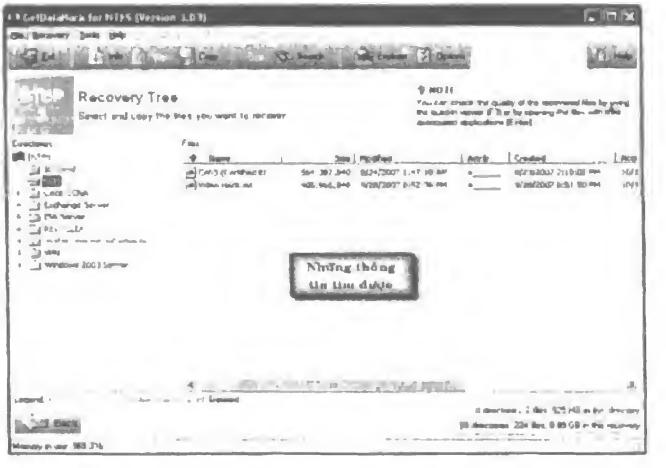
Hình 4.39: *Đang tiến hành quá trình tìm kiếm.*

3. Nhấp chọn vào file hệ thống muốn phục hồi, sau đó nhấp **Next** để tiếp tục (xem hình 4.40).



Hình 4.40: *Chọn file hệ thống muốn phục hồi.*

4. Sau khi nhấp nút **Next**, chương trình sẽ hiển thị những thông tin mà nó tìm được như hình 4.41.



Hình 4.41: *Những thông tin tìm được.*

5. Tiếp theo, bạn thực hiện khôi phục dữ liệu như những mục trước.

Hướng dẫn thêm:

- **File Allocation Table (FAT):** Một bảng trên đĩa mềm hay đĩa cứng dùng để lưu giữ thông tin về cách thức các tập tin được lưu trữ như thế nào trong các cluster riêng biệt, không nhất thiết liền nhau. Bảng phân bố tập dùng một phương pháp đơn giản. Với FAT cluster đầu tiên là địa chỉ của cluster thứ hai được sử dụng để lưu trữ tập đó. Trong mục FAT đối với cluster thứ hai là địa chỉ của cluster thứ ba, cứ như thế tiếp tục cho đến khoản mục của cluster cuối cùng chứa mã kết thúc của tập. Vì chỉ có duy nhất

bảng này cho biết cách tìm dữ liệu trên đĩa, cho nên DOS sẽ thành lập và duy trì hai bản sao của FAT để đề phòng một bị hỏng.

- **New Technology File System (NTFS):** Là công nghệ mới dùng để quản lý tập tin trên Windows. NTFS được thiết kế cho các thao tác tập tin nhanh trên các ổ đĩa cứng có dung lượng lớn. NTFS bao gồm một hệ thống phục hồi tập tin và các thuộc tính được xây dựng sẵn để giải quyết an toàn và điều khiển truy xuất. Khi bạn định dạng một phân vùng (partition) trên một ổ đĩa sử dụng hệ thống tập tin NTFS, thì phân vùng này được khởi tạo như là một volume của NTFS. Volume này chứa MFT (master file table), chứa thông tin về từng tập tin có trong volume này. Thông tin này được lưu trữ trong các mẫu tin có kích thước 2,048 byte và hoạt động giống như một cơ sở dữ liệu quan hệ. Các tập tin được xác định bởi một con số, số này phụ thuộc vào vị trí của tập tin trong MFT và một số tuần tự đặc biệt.

IV. Get Data Back for FAT

Đây là chương trình cho phép tìm lại tất cả các dữ liệu mà sau khi bạn đã Fdisk, Format, hay sự tấn công của virus, worm, lỗi phần mềm hoặc những tập tin đã xóa trên những ổ đĩa có phân vùng được định dạng theo kiểu FAT.

Chương trình tương thích với Windows 2K/XP. Sau khi giải nén và cài đặt chương trình, bạn thực hiện như sau:

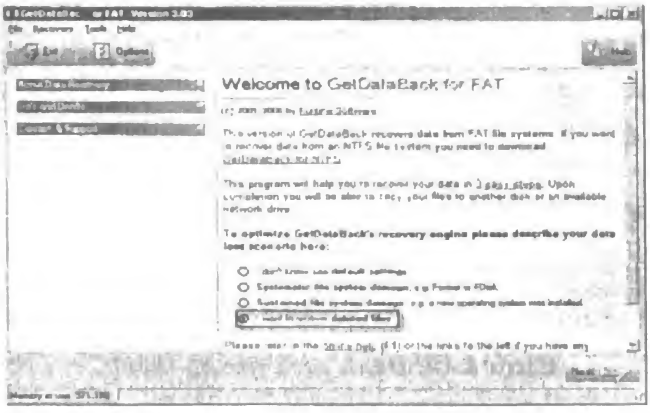
1. Tìm lại tập tin đã xóa

Việc xóa nhầm những tập tin quan trọng là điều không thể tránh khỏi đối với những ai đã và đang sử dụng máy tính. Việc này sẽ không đáng nói khi những tập tin mà bạn xóa không quan trọng, nhưng nếu ngược lại, những tập tin bạn xóa nhầm lại là những tài liệu rất quan trọng liên quan đến công việc và sự phát triển của công ty.

Tìm lại những tập tin không khó, trong mục này giới thiệu đến bạn một số phương pháp giúp tìm nhanh lại những tập tin mà bạn đã xóa nhầm trên phân vùng có định dạng FAT32. Để thực hiện bạn làm như sau:

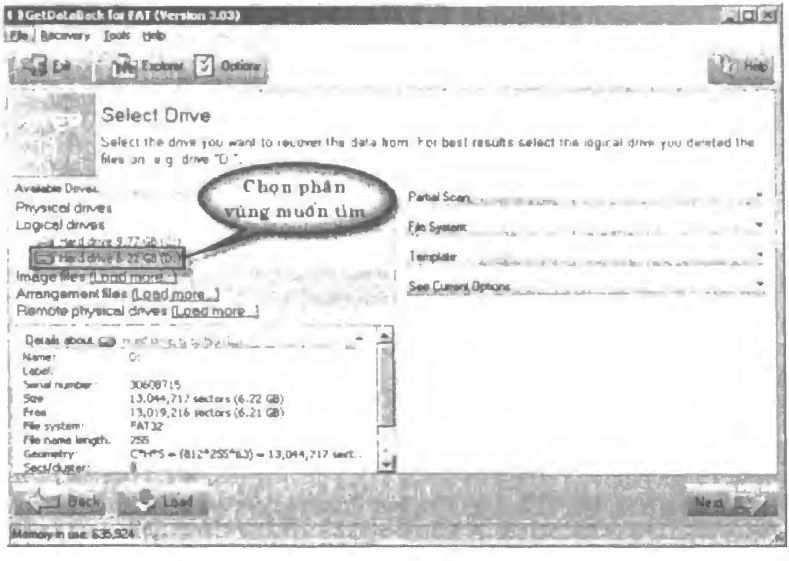
1. Vào **Start > Programs > Runtime Software > Get Data Back for FAT** để mở chương trình.

2. Tại giao diện chính của chương trình, nhấp chọn vào mục **I want to recovery deleted files**, sau đó nhấp **Next** để tiếp tục (xem hình 4.42).



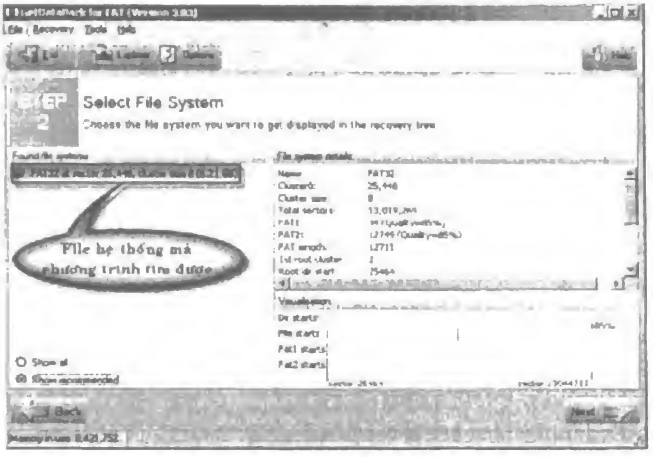
Hình 4.42: *Chọn I want to recovery deleted files.*

3. Nhấp chọn vào phân vùng muốn tìm, sau đó nhấp **Next** để tiếp tục. Do chương trình này chỉ tìm được những tập tin trên phân vùng FAT, do vậy ta chọn phân vùng **D** trong máy tính (xem hình 4.43).



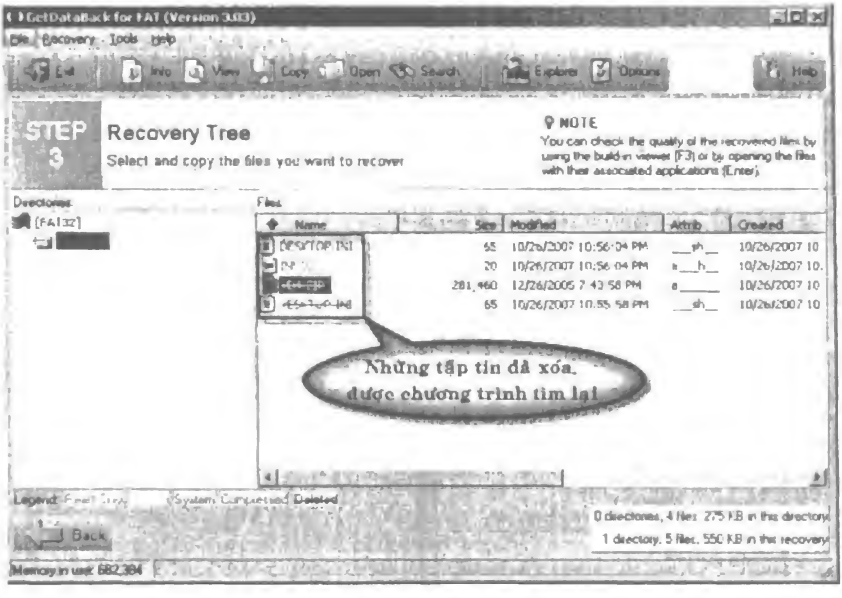
Hình 4.43: *Chọn phân vùng phục hồi dữ liệu.*

4. Chương trình sẽ liệt kê những tập tin hệ thống mà nó tìm được. Bạn nhấp vào tập tin muốn phục hồi sau đó nhấp **Next** để tiếp tục (xem hình 4.44).



Hình 4.44: *Danh sách file hệ thống.*

5. Trong mục này ta phục hồi tập tin hệ thống theo phương thức tìm lại những tập tin, thư mục đã bị xóa. Do vậy chương trình sẽ hiển thị danh sách các tập tin mà nó tìm được (xem hình 4.45).



Hình 4.45: *Các tập tin mà chương trình tìm được.*

6. Nhấp vào tập tin muốn phục hồi, sau đó nhấn phím **F5** trên bàn phím để thực hiện copy và mở của sổ Copy files.

7. Tại cửa sổ này, nhấp nút **Browse for directory** để chỉ ra đường dẫn lưu tập tin mà bạn muốn phục hồi, mặc định đường dẫn này là

C:\Document and Settings\Administrator. Trong đó Administrator là tài khoản mà bạn đăng nhập vào máy tính (xem hình 4.46).

Hình 4.46: *Chọn đường dẫn lưu tập tin phục hồi.*

Đến đây ta đã hoàn thành công việc phục hồi lại những tập tin đã xóa mất, bạn có thể khám phá thêm nhiều chức năng khác khi sử dụng chương trình.

V. Data Doctor Recovery - NTFS-FAT

Chương trình này có những chức năng sau:

- Khôi phục phân vùng bị hư hại hoặc bị xóa.
- Tìm lại những tập tin hoặc thư mục bị mất.
- Phục hồi dữ liệu khi Master Boot Record (MBR) bị mất.
- Phục hồi dữ liệu bị mất, sau khi đĩa cứng bị format.
- Tìm lại dữ liệu trong trường hợp bị mất do virus.
- Hỗ trợ những tập tin có tên dài.
- Phục hồi lại những tập tin từ những phân vùng bị format hoặc định dạng dưới bất kỳ một tham số nào.
- Phục hồi lại dữ liệu ngay cả khi những MFT bị hư hỏng
- Hỗ trợ IDE, EIDE, SCSI và SATA, PEN, ZIP drives.

Chương trình này hỗ trợ phục hồi trên hai loại phân vùng, đó là NTFS và FAT.

Sau khi giải nén và cài đặt vào máy tính, bạn thực hiện như sau:

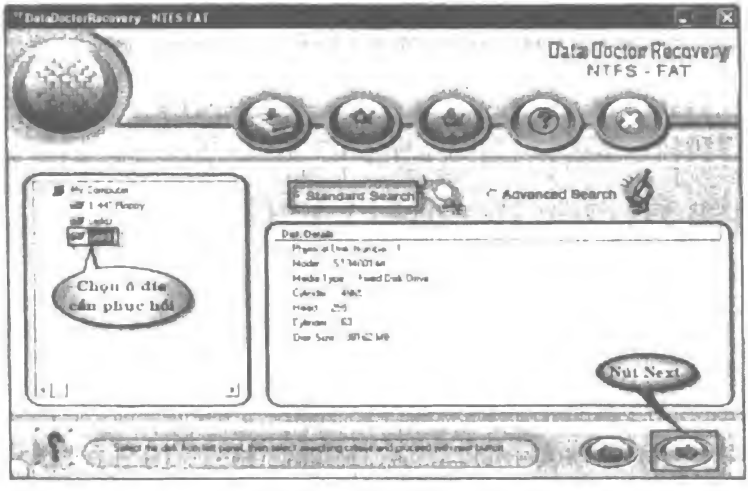
1. Standard Search

Tiện ích này cho phép bạn thực hiện những chức năng tìm kiếm và phục hồi căn bản, cách thực hiện như sau:

1. Vào **Start > Programs > Data Doctor Recovery > NTFS - FAT > Data Doctor Recovery - NTFS-FAT** để mở chương trình.

2. Nhấp chọn ổ đĩa muốn phục hồi, tiếp theo chọn **Standard Search**, sau đó nhấp **Next** để tiếp tục.

Chương trình sẽ tiến hành tìm trên ổ đĩa bạn vừa chọn có bao nhiêu phân vùng và hiển thị chúng theo danh sách với tên bắt đầu từ Partition - 1 đến Partition - n, ngoài ra nó còn hiển thị định dạng của phân vùng là NTFS hay FAT (xem hình 4.47).



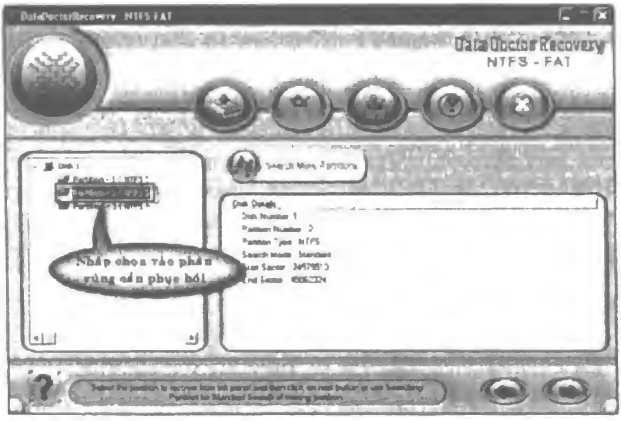
Hình 4.47: *Giao diện chính của chương trình.*

3. Nhấp chọn vào phân vùng muốn phục hồi, sau đó nhấp **Next** để tiếp tục (xem hình 4.48).

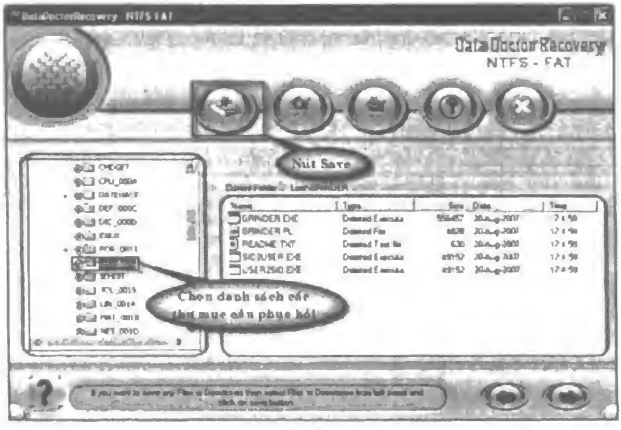
4. Nhấp chọn vào thư mục muốn phục hồi, sau đó nhấp nút **Save** để lưu thông tin.

Danh sách các tập tin thư mục được tổ chức thành danh sách trong cây thư mục (xem hình 4.49).

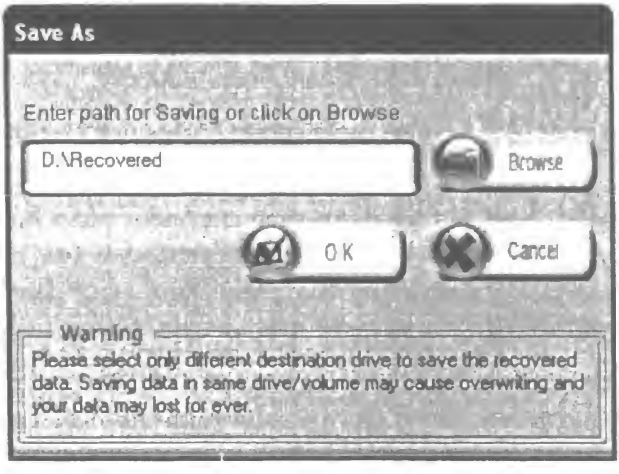
5. Nhấp nút **Browse** để chọn đường dẫn lưu thông tin phục hồi, sau đó nhấp **OK** để thực hiện (xem hình 4.50).



Hình 4.48: *Chọn phân vùng phục hồi.*



Hình 4.49: *Nhấp chọn thư mục muốn phục hồi.*



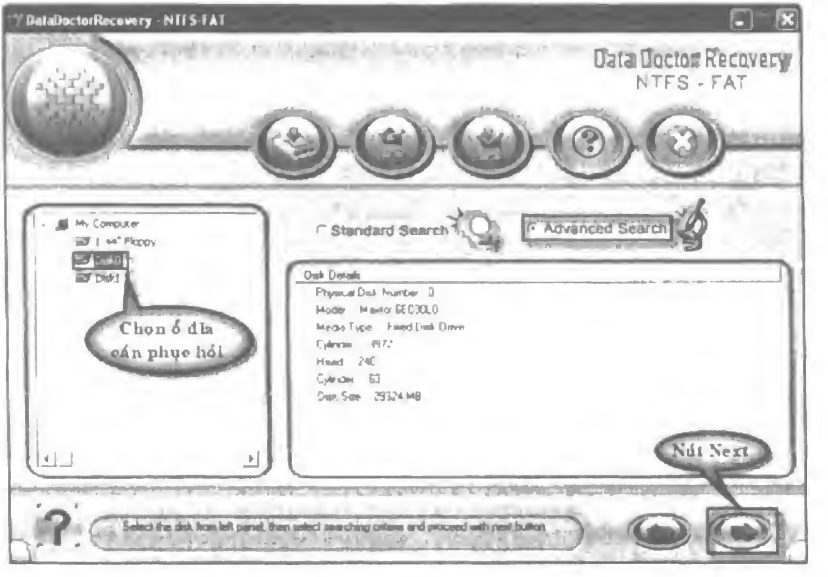
Hình 4.50: *Chọn đường dẫn lưu thông tin.*

Sau khi phục hồi xong, nếu muốn quay lại mục trước để tìm những tập tin, thư mục khác để phục hồi tiếp thì bạn nhấp nút **Back** để quay lại. Chương trình có giao diện đồ họa tương đối trực quan, mỗi biểu tượng của các mục tương ứng với một tiện ích nhất định.

2. Advanced Search

Tiện ích này cho phép tìm những tập tin, thư mục, bị mất do các nguyên nhân như: Format, Fdisk,..

1. Trên trang giao diện chính của chương trình, nhấp chọn ổ đĩa muốn phục hồi, sau đó nhấp chọn vào mục **Advanced Search**, tiếp theo nhấp **Next** để tiếp tục (xem hình 4.51).



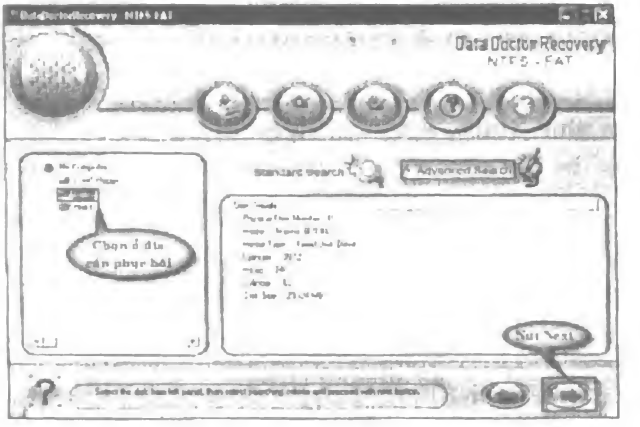
Hình 4.51: *Chọn ổ đĩa phục hồi.*

2. Nhấp chọn phân vùng muốn phục hồi, sau đó nhấp **Next** để thực hiện.

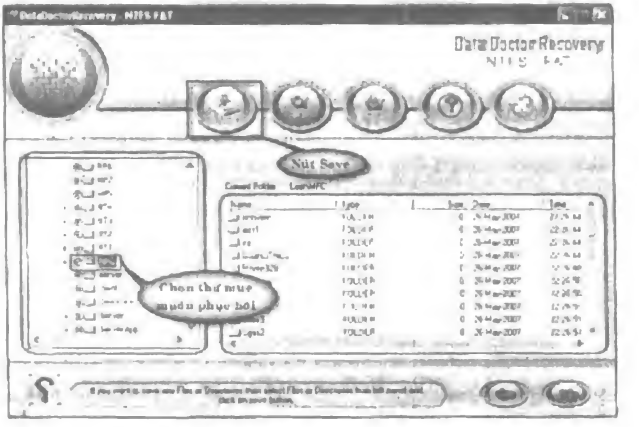
Chương trình sẽ liệt kê danh sách các phân vùng hiện có của ổ đĩa đã chọn, danh sách các phân vùng được tổ chức với tên từ Partition – 1 đến partition – n, và định dạng của phân vùng cũng được hiển thị theo (xem hình 4.52).

3. Nhấp chọn vào thư mục chứa các tập tin cần phục hồi, tiếp theo nhấp nút **Save** để lưu tập tin (xem hình 4.53).

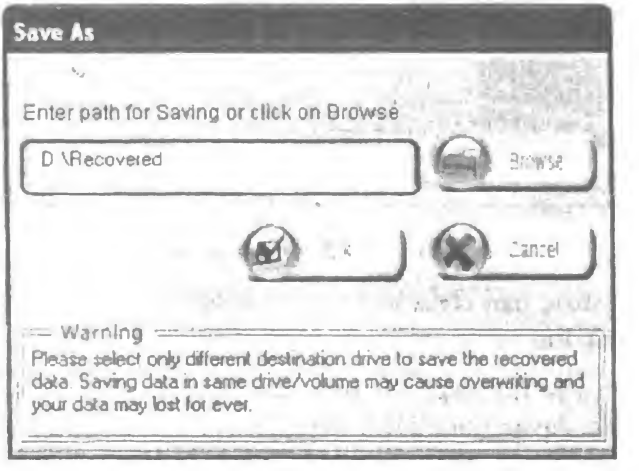
4. Nhấp nút **Browse** để chọn đường dẫn lưu thông tin phục hồi, sau đó nhấp **OK** để áp dụng (xem hình 4.54).



Hình 4.52: *Chọn phân vùng cần phục hồi.*



Hình 4.53: *Chọn thư mục cần phục hồi.*



Hình 4.54: *Chọn đường dẫn lưu thông tin.*

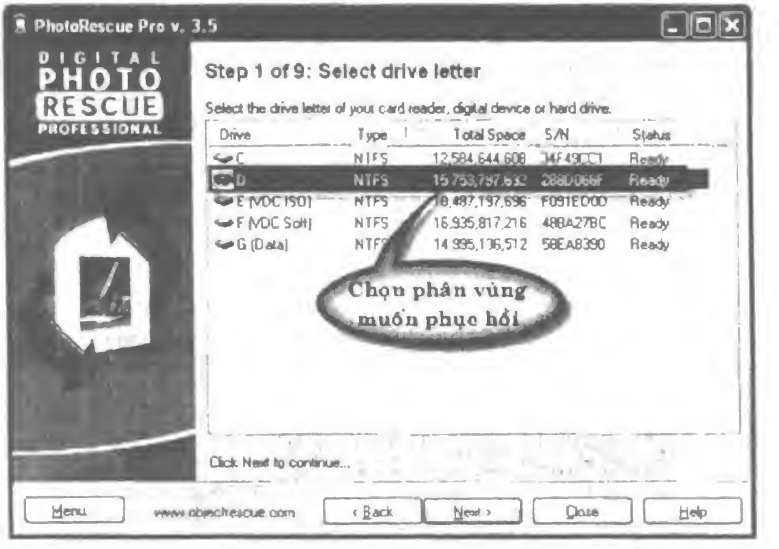
VI. PhotoRescue Professional

Chương trình cho phép tìm lại tất cả những dữ liệu liên quan đến các file Media như: Video, Audio, Images, bị mất do các nguyên nhân như: Những tập tin bị xóa, đĩa cứng bị format, fdisk, hoặc những files bị mất do những chương trình phá hoại dữ liệu.

Chương trình tương thích với mọi phiên bản của Windows. Sau khi giải nén và cài đặt chương trình, bạn thực hiện như sau:

1. Vào **Start > Programs > PhotoRescue Pro > PhotoRescue Professional** để mở chương trình.
2. Hộp thoại đầu tiên xuất hiện, bạn nhấp **Next** để tiếp tục.
3. Tiếp theo, nhấp chọn phân vùng muốn phục hồi, sau đó nhấp **Next** để tiếp tục.

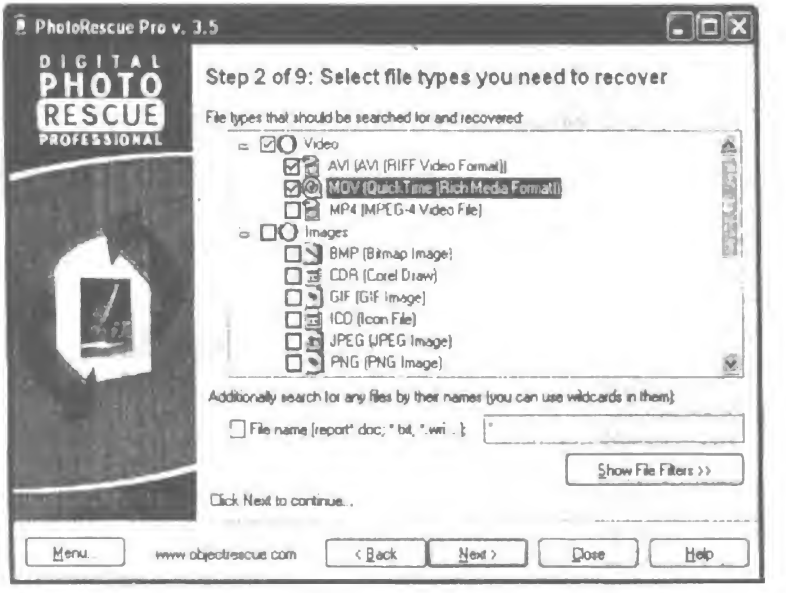
Chương trình sẽ liệt kê danh sách các phân vùng của tất cả các ổ đĩa trong máy tính thành một danh sách (xem hình 4.55).



Hình 4.55: *Chọn phân vùng cần phục hồi.*

4. Tiếp theo, bạn chọn loại tập tin muốn phục hồi, sau đó nhấp **Next** để tiếp tục.

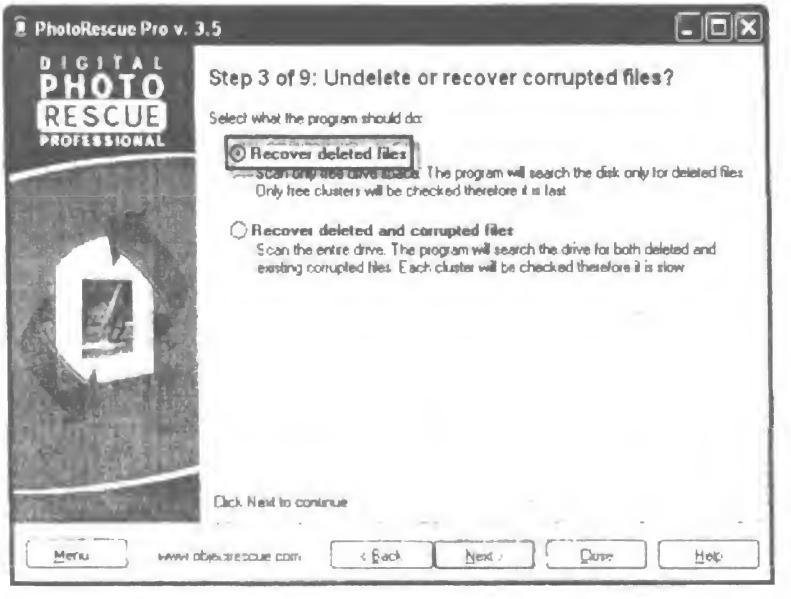
Danh sách các tập tin được tổ chức thành 3 nhóm chính đó là Video, Images, Audio (xem hình 4.56).



Hình 4.56: *Chọn loại tập tin muốn phục hồi.*

5. Nhấp chọn vào mục **Recovery deleted files**, sau đó nhấp **Next** để tiếp tục.

Mục này cho phép bạn phục hồi những tập tin media bị xóa (xem hình 4.57).

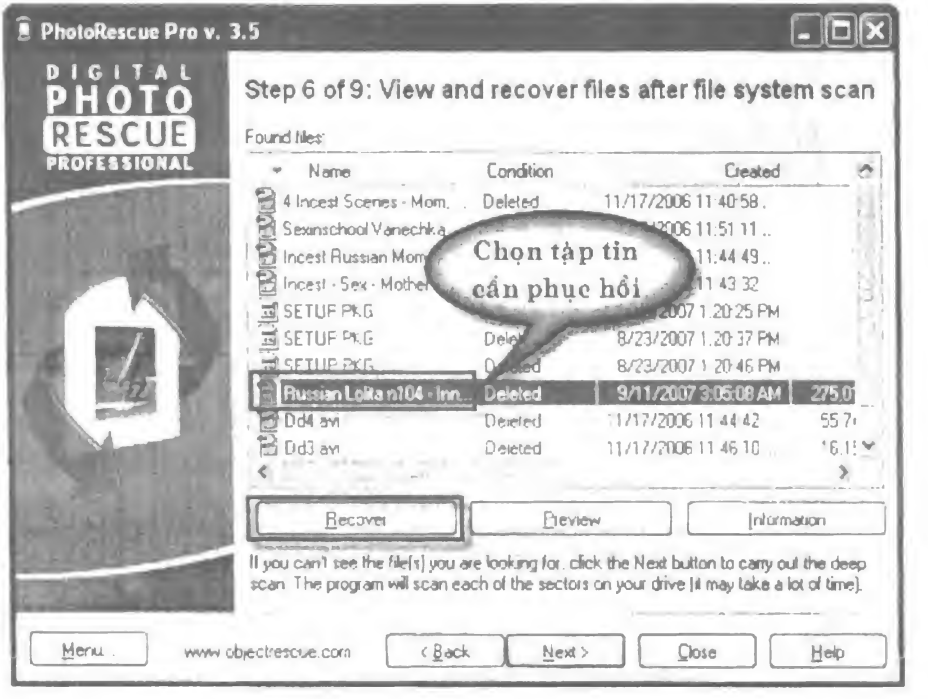


Hình 4.57: *Phục hồi những tập tin bị xóa.*

6. Nhấp nút **Browse** để chọn đường dẫn lưu những tập tin cần phục hồi, sau đó nhấp **Next** để thực hiện.

7. Trong trang Step 5 of 9: Scan the file system, bạn nhấp **Next** để tiếp tục.

8. Danh sách các tập tin được hiển thị trong danh sách, bạn chọn tập tin muốn phục hồi sau đó nhấp nút **Recovery** để thực hiện phục hồi từng tập tin một (xem hình 4.58).



Hình 4.58: *Chọn tập tin muốn phục hồi.*

9. Nhấp **Next** để tiếp tục.

Khi bạn nhấp Next thì tất cả những tập tin trong danh sách đều được phục hồi vào trong thư mục mà bạn đã chọn ở bước 6.

10. Danh sách các tập tin được hiển thị, bạn nhấp **Next** để tiếp tục, sau đó nhấp nút **Close** để hoàn thành.

Lúc này bạn có thể di chuyển đến thư mục mà bạn đã chọn ở bước 6 để kiểm tra những thông tin đã phục hồi.

VII. Một số chương trình phục hồi dữ liệu khác

1. Active@ Undelete

Chương trình cho phép bạn tìm nhanh những thông tin bị mất trong đĩa cứng của bạn. Những thông tin tìm được là những thông tin bị mất do các nguyên nhân như: Những tập tin đã bị xóa, ổ cứng bị Fdisk hoặc Format, hay do sự phá hoại của các chương trình phá hoại dữ liệu như: virus, worm...

Sau khi giải nén và cài đặt chương trình, bạn thực hiện tương tự như những phần trước để phục hồi.

2. Final Recovery

Chương trình này cũng tích hợp đầy đủ các phương thức phục hồi dữ liệu như những chương trình đã giới thiệu trong các phần trước của chương. Sau khi giải nén và cài đặt chương trình, bạn thực hiện tương tự như các mục trước để phục hồi.

3. Power Data Recovery

Chương trình này có dung lượng tương đối khiêm tốn và không cần cài đặt (đối với phiên bản 3.1.1, nhưng với phiên bản 3.1.0 thì ta vẫn phải cài đặt bình thường), thế nhưng chức năng mà nó mạng lại rất lớn, nó có thể tìm lại hầu như là tất cả những thông tin bị mất trên đĩa cứng của bạn.

4. Data Recovery Wizard Professional 3.3.4

Đây là chương trình được thiết kế chuyên cho việc phục hồi dữ liệu, nó có thể nhanh chóng giúp bạn tìm ngay lại những tập tin mà bạn đã vô tình xóa nhầm, hay những tập nằm trong những phân vùng đã bị format. Tất cả những tập tin có thể được tìm lại và phục hồi nguyên vẹn.

Chương trình tương thích với mọi Windows, dung lượng nhỏ gọn, giao diện thân thiện, làm việc hiệu quả. Sau khi giải nén và cài đặt vào máy tính, bạn thực hiện tương tự như những mục trước để phục hồi.

5. Recover My Files

Đây là chương trình có giao diện tương đối thân thiện và trực quan, nó hỗ trợ tìm lại những tập tin, thư mục trên hai loại phân vùng FAT và NTFS, những phân vùng bị format hoặc những tập tin bị xóa có thể được tìm lại một cách nhanh chóng.

Chương trình tương thích với mọi Windows, dung lượng nhỏ gọn.

6. Partition Recovery 2.0

Đây là tiện ích giúp tìm lại những phân vùng đã mất do các nguyên nhân sau:

- Phân vùng bị xóa.
- Phân vùng bị mất do bị lỗi bảng tham số đĩa.
- Phân vùng bị mất do virus hoặc những nguyên nhân khác.

Chương trình hỗ trợ phục hồi trên nhiều loại file hệ thống như FAT 12, FAT 16, FAT 32, NTFS, NTFS5, HPFS, tiện ích này tương thích với mọi Windows, dung lượng nhỏ gọn, giao diện thân thiện và dễ sử dụng.

7. BadCopy Pro

Chương trình có một số chức năng sau:

- Sửa chữa và phục hồi những dữ liệu trên đĩa mềm bị hư.
- Sửa chữa và phục hồi dữ liệu trên tất cả các loại đĩa CD – ROM, CD – R, CD – RW.
- Phục hồi tất cả dữ liệu bị mất trên các thiết bị lưu trữ như CD, đĩa mềm.
- Phục hồi những hình ảnh được lưu trữ trên các thiết bị như Camera...

Chương trình tương thích với mọi phiên bản của Windows.

Chương 5:

AN TOÀN DỮ LIỆU

- **Tìm hiểu về an toàn dữ liệu.**
- **BPS Data Shredder.**
- **Track Eraser Pro.**
- **Một số chương trình bảo mật khác.**

Dữ liệu là một trong những vấn đề sống còn của doanh nghiệp, vì vậy, an toàn dữ liệu luôn được đặt lên hàng đầu.

Dữ liệu được tồn tại và lưu trữ ở nhiều dạng khác nhau, có thể là: Danh sách khách hàng, những tài liệu mật liên quan đến chiến lược của công ty, dữ liệu riêng tư, hay bất kỳ một tài liệu nào mà bạn hoặc công ty không muốn cho những người không phận sự biết.

Dữ liệu được lưu trên những thiết bị như: Đĩa cứng của máy tính, USB Flash Drive hay Floppy, gọi chung mà Media. Tất cả những tài liệu, nếu tồn tại trên những thiết bị lưu trữ, hacker có thể khai thác và phục hồi lại một cách nhanh chóng và toàn diện, mặc dù bạn đã xóa nó.

Ngoài ra, khi thực hiện trên máy tính, như xem phim, hình ảnh hay lướt web,..., tất cả những thông tin cũng như hoạt động của bạn đều được máy tính, trình duyệt ghi lại và lưu lại ở những nơi như: Registry, Cookies, History, Temporary files,..., những thông tin này nhiều khi cũng gây rất nhiều những rắc rối cho bạn như: Tài khoản ngân hàng bị mất, password bị đổi.

Chương này giới thiệu một số cách giúp xóa sạch những dữ liệu khi bạn không dùng đến hoặc khi chuyển những thiết bị lưu trữ cho những đối tượng người dùng khác. Ngoài ra, chương này còn giúp bạn xóa sạch những dấu vết khi bạn thao tác trên máy tính.

I. Tìm hiểu về an toàn dữ liệu

1. Cảnh báo về việc xóa dữ liệu

Thật sai lầm khi nghĩ rằng chỉ cần delete hay format ổ cứng là có thể xóa sạch dữ liệu trong đĩa cứng hay flash drive hoặc bất kỳ một thiết bị lưu trữ nào.

Bạn thường cho bạn bè hay đồng nghiệp mượn ổ đĩa flash và bạn yên tâm rằng mình đã delete tất cả các tập tin dữ liệu và format ổ đĩa của mình rồi. Bạn thường thuê máy tính để làm việc khi trả máy bạn chỉ cần delete là yên tâm và khi đang làm việc thì ổ cứng của bạn có sự cố và bạn đem đi bảo hành, nhưng bạn có biết rằng chỉ với vài thao tác đơn giản thì cái dữ liệu mà bạn cho rằng chỉ có bạn mới có quyền truy cập bây giờ đã được chia sẻ cho người khác. Thật nguy hiểm nếu dữ liệu đó là dữ liệu mật của công ty, thông tin khách hàng, hay những thông tin riêng tư của bạn.

2. Đôi điều về lệnh Delete và Format

Delete hay Format không thể tẩy sạch dữ liệu:

Các chương trình ứng dụng thường tạo ra các tập tin được lưu trữ trên đĩa cứng hay các loại đĩa khác như đĩa mềm (floppy), CD, DVD kể cả băng từ và flash drive. Khi cảm thấy không cần một tập tin (file) hay thư mục (folder) nào đó nữa thì người dùng sẽ xóa tập tin đó đi. Đối với một số người thì tập tin hay thư mục đó hoàn toàn biến mất vĩnh viễn và không thể phục hồi, nhưng đối với một số khác thì không. Người dùng nên biết rằng để chạy tốt thì Windows và các trình ứng dụng đã sinh ra các tập tin có nội dung tương tự và cũng lưu trên ổ cứng, chẳng hạn: Windows tạo ra các Swap files và Page files để hỗ trợ bộ nhớ ảo, Temporary files làm lưới dữ liệu an toàn, Printer Spool Files để thực hiện in nhanh và ổn định hơn, Metadata (siêu dữ liệu) là những dữ liệu lưu trữ thông tin về các loại dữ liệu khác. Như vậy, mọi dữ liệu từng được lưu trữ vào ổ cứng vẫn còn dù người ta có Delete, ném nó vào thùng rác (Recycle bin) hay Format và phân vùng đĩa cứng lại. Tuy vậy lệnh Delete hay Format vẫn được các hệ điều hành như Windows 9x /2000/ XP ưu ái vì nó tiết kiệm được thời gian "xóa" dữ liệu.

Thực chất với lệnh Delete người dùng chỉ xóa đường dẫn tới dữ liệu chứ không thể xóa thông tin ra khỏi đĩa cứng, điều này cũng giống như việc bạn chỉ bỏ trang mục lục của cuốn sách mà chưa hủy phần nội dung của cuốn sách.

3. Làm sao để bảo mật thông tin

Vậy để bảo mật thông tin, thông báo nội bộ, các dự án, số liệu tài chính, dữ liệu khách hàng... bạn cần những phần mềm tẩy sạch (santinize) dữ liệu an toàn.

4. Các phương pháp tẩy sạch dữ liệu an toàn

Hiện nay hầu hết các phần mềm hỗ trợ tẩy sạch dữ liệu được chạy trên nền DOS nên rất kém thân thiện với người dùng. Cũng có một số phần mềm chạy trên Windows 9x/2000/XP dễ dùng hơn. Những mục tiếp theo của chương này sẽ giới thiệu đến các bạn những phần mềm giúp tẩy sạch dữ liệu an toàn chạy trên môi trường Windows. Trước tiên chúng ta hãy tìm hiểu một số phương pháp tẩy sạch dữ liệu.

- **Single pass** (xóa một lần): Toàn bộ khu vực dữ liệu trên ổ cứng được ghi đè (overwrite) bằng ký tự 0 hoặc 1 hoặc dữ liệu ngẫu nhiên (Random data).
- **DoD**: Đây là phương pháp của Bộ Quốc Phòng Mỹ, là biến thể của phương pháp "Single pass" với số lần ghi đè (overwrite) là 7, luân phiên overwrite bằng ký tự 0 hoặc 1 hay ký tự ngẫu nhiên, theo tài liệu hướng dẫn 5220.22-M còn gọi là NISPOM (National Industrial Security Program Operating Manual). Để tẩy sạch (santinize) đĩa cần phải kết hợp với các phương pháp sau:
  - **Khử từ** (Degauss): Dùng từ trường để tái lập lại các lá từ trong thiết bị bằng phương pháp khử từ loại I hay II.
  - Overwrite tại mọi địa chỉ trên ổ cứng bằng một ký tự kể cả các thành phần liên quan, rồi tiếp tục overwrite bằng ký tự ngẫu nhiên, sau đó kiểm tra xác nhận (verify). Tuy nhiên Bộ Quốc Phòng Mỹ cũng nói rằng phương pháp này không dùng để xóa thông tin tuyệt mật (Top Secret Information).
  - Hủy thiết bị lưu trữ thông tin bao gồm tháo rã mọi thành phần của thiết bị lưu trữ thông tin (Disintegrate), đốt hủy (incinerate), nghiền thành bột (pulverize), cắt vụn (shred), làm tan chảy bằng nhiệt độ (smelt).
- **Guttmann:** Dữ liệu được overwrite 35 lần, phương pháp này dùng ký tự ngẫu nhiên để overwrite và áp dụng các thuật toán mã hóa của nhiều hãng sản xuất đĩa cứng như: RLL (Run Length limited), MFM (Modifiel Friquency Modulation), PRML...

Phương pháp overwrite tùy chọn từ 1-99 lần.

Lưu ý:

Cơ sở duy nhất để ngăn chặn phục hồi dữ liệu là overwrite, song phải overwrite bao nhiêu lần mới đủ? Có những người tin rằng chỉ cần overwrite một lần là đủ, thật ra overwrite càng nhiều lần thì càng giảm đi cơ hội phục hồi dữ liệu.

Trong mục tiếp theo chúng tôi sẽ giới thiệu đến bạn một số phần mềm giúp bạn tẩy sạch dữ liệu an toàn.

II. BPS Data Shredder

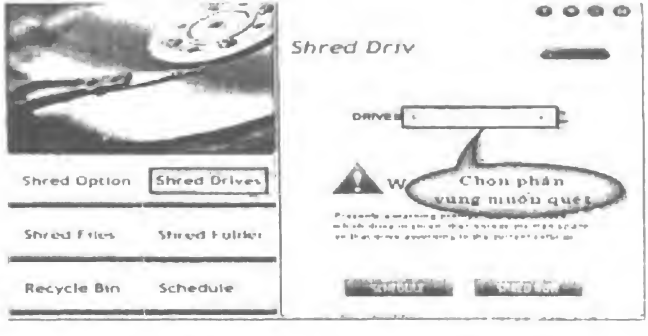
Là chương trình phá hủy các dữ liệu hợp pháp, giải phóng bộ nhớ, không gian đĩa, và Recycle bin. Điều này có nghĩa là nội dung dữ liệu của bạn sẽ bị ghi đè lên bởi các bytes ngẫu nhiên. Dữ liệu vì vậy sẽ rất an toàn mà không cần áp dụng các biện pháp vật lý để phân hủy dữ liệu.

Bạn có thể download chương trình tại website www.minhkhai.com.vn, thư mục Chapter 5, sau khi giải nén và cài đặt, bạn thực hiện tẩy sạch như sau:

1. Shred Drives

Tiện ích này sẽ giúp giải phóng không gian đĩa cứng, và xóa sạch dữ liệu cần bảo mật, để thực hiện, bạn làm như sau:

1. Vào **Start > Programs > BulletProofSoft > BPS Data Shredder > BPS Data Shredder** để mở chương trình.
2. Tại giao diện chính của chương trình, nhấp chọn **Shred Drives**.
3. Trong trang Shred Drives, tại mục Drives, bạn chọn ổ đĩa mà bạn muốn thực hiện, sau đó nhấp **Shred Now** để tiếp tục (xem hình 5.1).

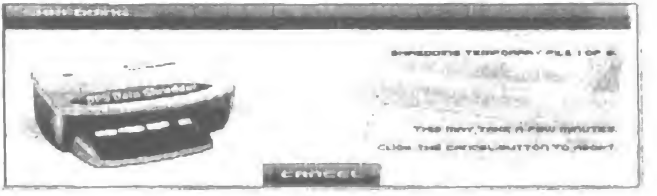


Hình 5.1: *Chọn phân vùng để quét.*

4. Tiếp theo, nhấp **OK** để thực hiện.

Chương trình xuất hiện thông báo về tình trạng của không gian đĩa và những thông tin khác.

5. Sau đó chương trình tiến hành xóa các mục trong phần vùng đã chỉ định, đợi khoảng 4 phút, tuy nhiên thời gian đợi tỷ lệ thuận với tổng dung lượng của các tập tin mà chúng ta đã chọn (xem hình 5.2).



Hình 5.2: *Quá trình xóa sạch dữ liệu.*

Nếu đợi lâu và không muốn thực hiện tiếp thao tác này nữa, bạn có thể nhấp nút **Cancel** để loại bỏ thao tác.

2. Shred Files

Mục này cho phép lựa chọn những tập tin mà bạn muốn tẩy sạch nó khỏi đĩa cứng của bạn, để thực hiện, bạn làm như sau:

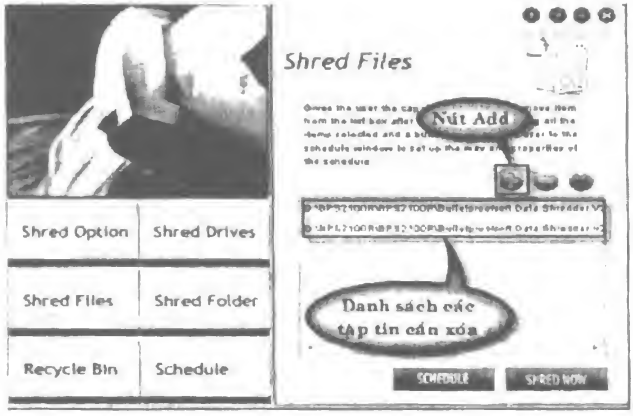
1. Tại giao diện chính của chương trình, nhấp vào **Shred Files**.
2. Trong trang Shred Files, bạn nhấp nút **Add** để chỉ định tập tin mà bạn muốn xóa.

Bạn có thể đưa nhiều files vào danh sách (xem hình 5.3).

Hình 5.3: *Chỉ định tập tin muốn xóa.*

3. Nhấp nút **Shred Now** để thực hiện.

Nếu không muốn xóa một tập tin nào đó trong danh sách, bạn có thể nhấp chọn vào tập tin đó, tiếp theo nhấp nút **Remove** để loại bỏ, nút Remove có biểu tượng hình dấu trừ (-), nút Add có biểu tượng hình dấu cộng (+) (xem hình 5.4).



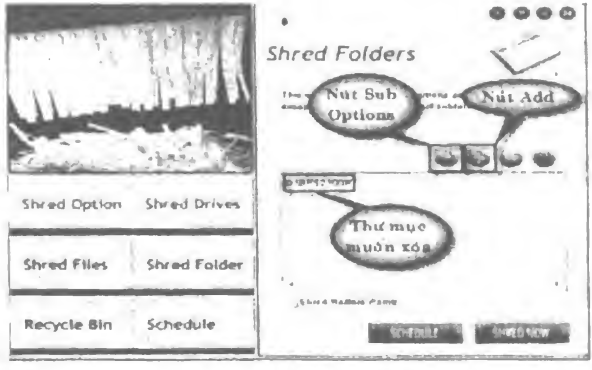
Hình 5.4: *Xóa tập tin trong danh sách.*

3. Shred Folder

Tiện ích này cho phép xóa tất cả các tập tin trong một thư mục được chỉ định, để thực hiện, bạn làm như sau:

1. Trong trang giao diện chính của chương trình, nhấp vào **Shred Folder**.
2. Nhấp nút **Add** để chỉ định thư mục mà bạn muốn xóa.

Bạn có thể chỉ định nhiều thư mục muốn xóa, bằng cách nhấp nút **Add** để đưa chúng vào danh sách (xem hình 5.5).

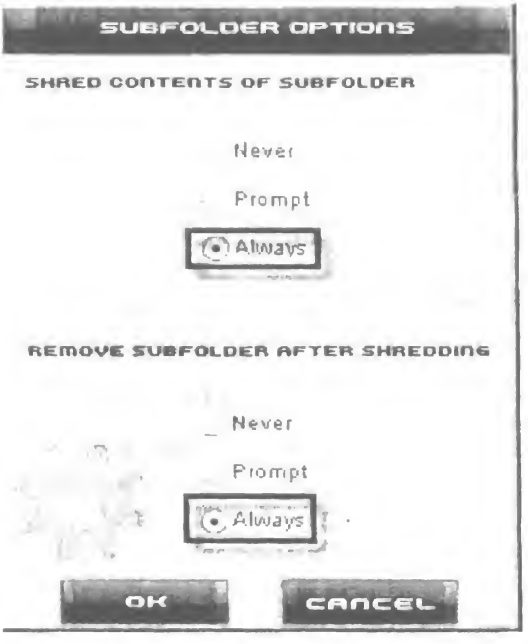


Hình 5.5: *Đưa các thư mục vào danh sách.*

3. Nhấp nút **Sub Options** và bạn nhấp chọn vào các mục sau:

- Nhấp chọn vào mục **Always** trong mục Shred contents of subfolder (xóa nội dung của thư mục con).
- Nhấp chọn vào mục **Always** trong mục Remove Subfolder affter Shred Dir.

Tiếp theo, nhấp **OK** để áp dụng (xem hình 5.6).



Hình 5.6: *Thiết lập trong hộp thoại Subfolder Options.*

4. Tại trang Shred Folders, nhấp nút **Shred Now** để thực hiện.

Sau khi nhấp nút Shred Now, chương trình sẽ yêu cầu xác nhận, bạn nhấp **Yes** để xác nhận.

4. Shred Recycle bin

Mục này cho phép bạn xóa tất cả những dữ liệu đã đưa vào Recycle bin, để thực hiện bạn làm như sau:

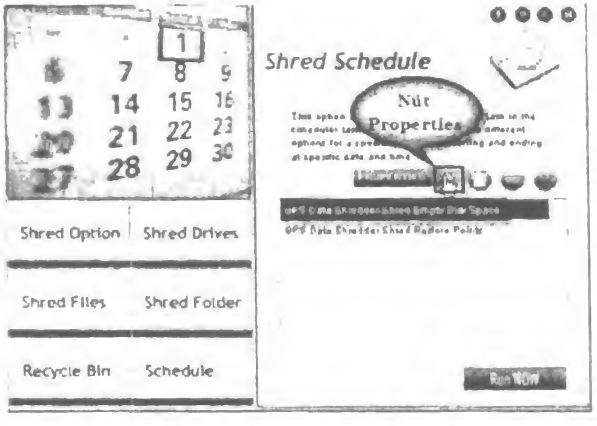
1. Trên trang giao diện chính của chương trình, nhấp **Recycle bin**.
2. Trong trang Shred Recycle Bin, nhấp nút **Shred Now** để thực hiện. Chương trình yêu cầu xác nhận, nhấp **Yes** để thực hiện (xem hình 5.7).

Hình 5.7: *Xóa sạch dữ liệu trong Recycle Bin.*

5. Schedule

Mục này cho phép lập lịch cho hoạt động của chương trình, để thực hiện, bạn làm như sau:

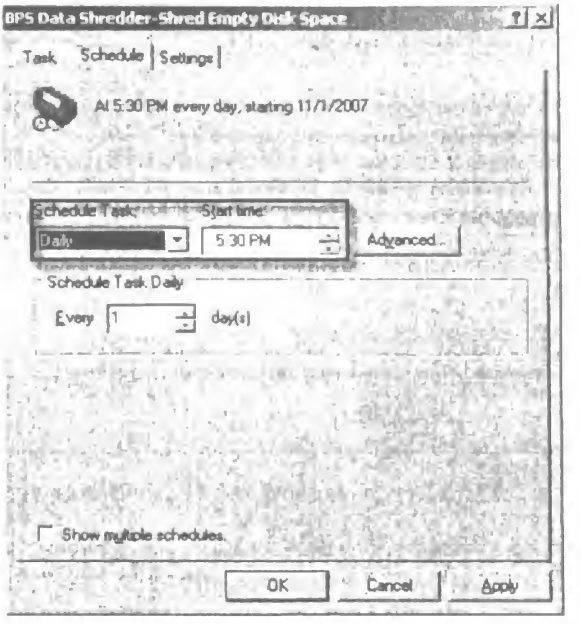
1. Trên giao diện chính của chương trình, nhấp vào **Schedule**.
2. Trong trang Shred Schedule, nhấp chọn vào mục **BPS Data Shredder - Shred Empty Disk Space**, sau đó nhấp nút **Properties** (xem hình 5.8).



Hình 5.8: *Lập lịch hoạt động cho chương trình.*

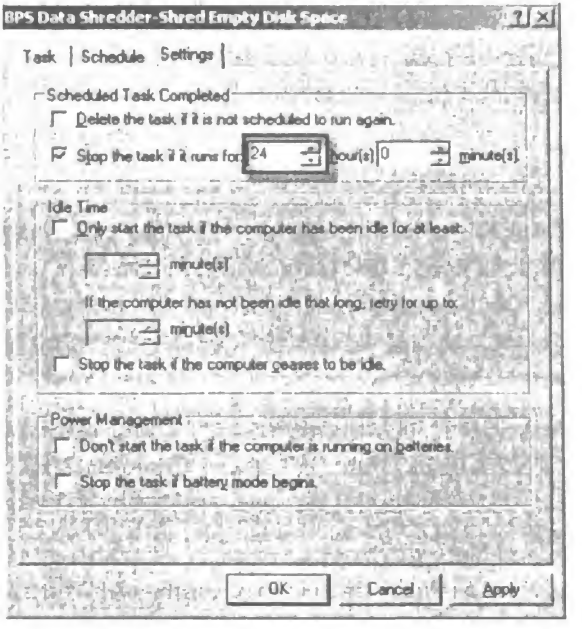
3. Nhấp chọn thẻ **Schedule**, trong mục Schedule Task, chọn **Daily**, tiếp theo, bạn nhập vào thời gian trong mục **Start time**.

Mục này cho phép chạy chương trình 1 ngày 1 lần tại thời gian mà bạn thiết lập trong mục mục Start time (xem hình 5.9).



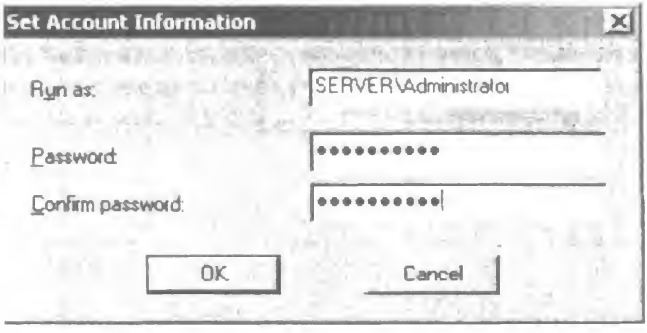
Hình 5.9: *Chọn thời gian khởi động chương trình.*

4. Chọn thẻ **Setting**, trong mục **Stop the task if it run for**, nhập vào thời gian tính bằng giờ và phút để dừng chương trình khi chạy quá thời gian quy định (xem hình 5.10).



Hình 5.10: *Những thiết lập trong thẻ Setting.*

5. Nhấp **OK** để áp dụng và hộp thoại Set Account Information xuất hiện. Bạn nhập vào password trong mục **Password** và nhập lại password trong mục **Confirm password** (xem hình 5.11).



Hình 5.11: *Nhập password truy cập chương trình.*

6. Trong trang Shred Schedule, nhấp **Run Now** để chạy chương trình.

Chương trình này tương thích với mọi Windows, và nguyên tắc hoạt động của nó là ghi đè các bytes ngẫu nhiên 0 và 1 lên địa chỉ chứa dữ liệu đã xóa

Như vậy, đến đây ta đã hoàn thành việc sử dụng và những thiết lập cần thiết cho việc thực thi và xóa sạch những dữ liệu mật của công ty, cũng như những dữ liệu riêng tư của bạn với chương trình BPS Data Shredder. Ngoài ra, chương trình còn rất nhiều tiện ích khác, bạn có thể khám phá thêm khi sử dụng chương trình.

III. Track Eraser Pro

Máy tính lưu trữ nhiều thông tin trên đĩa cứng và bất kỳ ai đăng nhập vào máy tính cũng có thể thấy những thông tin này. Hơn nữa, nếu sử dụng Internet thì những website mà bạn đã viếng thăm, những phim và hình ảnh đã xem, và bất kỳ những gì đã làm trên máy tính cũng có thể dễ dàng bị người khác biết.

Track Eraser Pro là chương trình được thiết kế để bảo vệ bằng cách xóa tất cả những dữ liệu ở History, Cache, Cookies, URL đã viếng thăm, bộ nhớ, index.dat từ trình duyệt của bạn và thư mục Temp của Windows, History của Run...

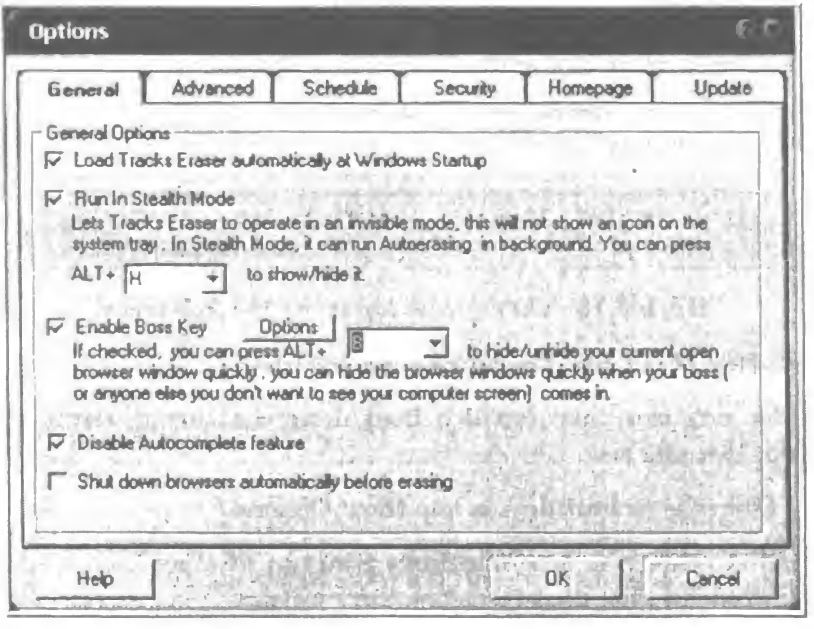
Sau khi giải nén và cài đặt chương trình, bạn thực hiện như sau:

1. Các tùy chọn của chương trình

1.1. Những mục trong thẻ Genaral

1. Vào **Start > Programs > Tracks Eraser Pro > Tracks Eraser Pro** để mở chương trình.
2. Tại giao diện chính của chương trình, nhấp nút **Options** để mở hộp thoại Options.
3. Tại hộp thoại Options, chọn thẻ **Genaral** và nhấp chọn vào các mục sau:

- **Load Tracks Eraser Automatically at Windows Startup:** nạp chương trình khi khởi động.
- **Run in Stealth Mode:** chạy chương trình ở dạng ẩn, tiếp theo bạn chọn phím mà bạn muốn kết hợp với phím chức năng Alt. Ví dụ, phím H.
- **Enable Boss Key:** cho phép ẩn, hiện trình duyệt hiện hành bằng cách kết hợp phím Alt với phím bạn chọn. Ví dụ, phím B để kết hợp với phím Alt.
- **Disable autocomplete feature:** vô hiệu hóa tính năng tự động thực hiện các chức năng (xem hình 5.12).

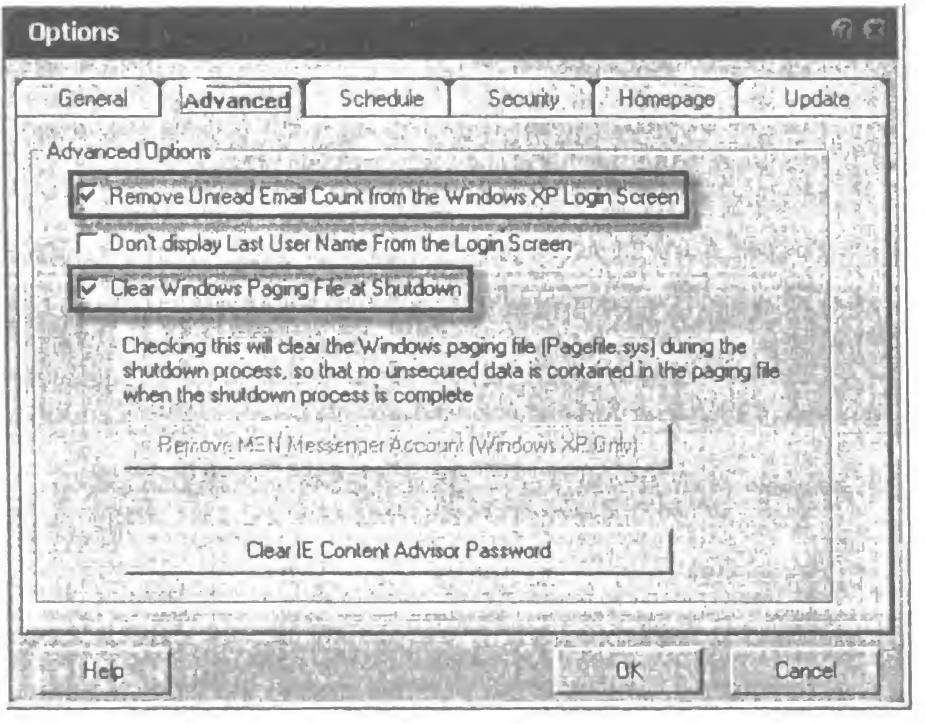


Hình 5.12: *Những tùy chọn trong thẻ Genaral.*

1.2. Những thiết lập trong thẻ Advanced

1. Trong hộp thoại Options, nhấp chọn thẻ **Advanced.**
2. Đánh dấu chọn vào các mục sau:

- **Remove Unread Email Count from the Windows XP Login Screen:** loại bỏ email không đọc từ màn hình đăng nhập của Windows XP.
- **Clear Windows Paging File at Shutdown:** xóa sạch nội dung file Pagefile.sys tại thời điểm Shutdown (xem hình 5.13).



Hình 5.13: *Những thiết lập trong thẻ Advanced.*

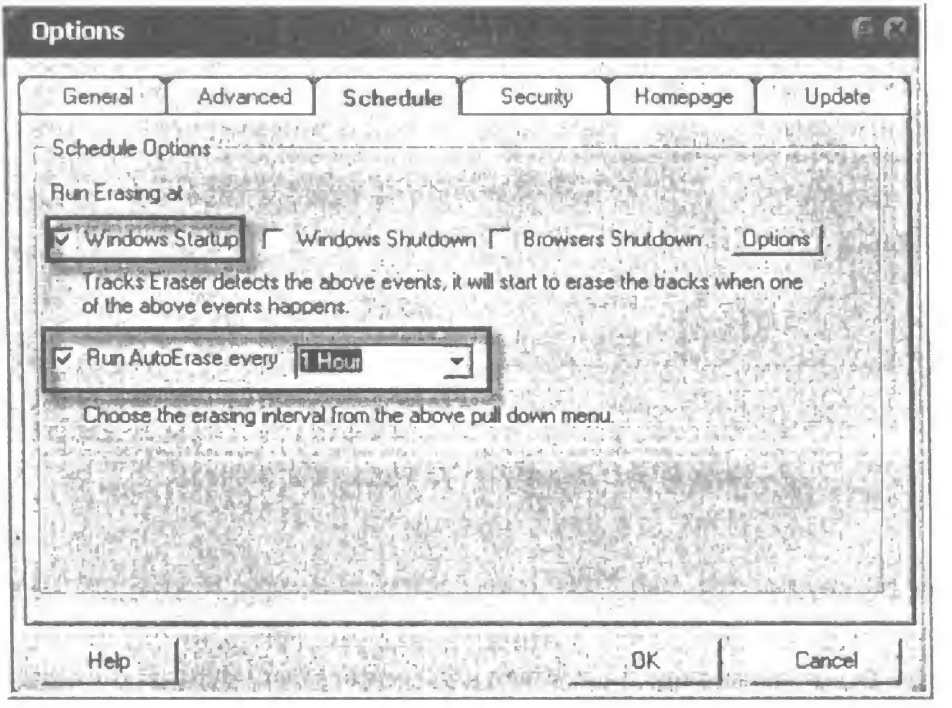
1.3. Những thiết lập trong thẻ Schedule

Mục này cho phép lập lịch hoạt động cho chương trình, để thực hiện, bạn làm như sau:

1. Chọn thẻ **Schedule** của hộp thoại Options.
2. Nhấp chọn vào mục **Windows Startup** để chạy chương trình khi Windows khởi động.

3. Nhấp chọn vào mục **Run AutoErase every** và chọn thời gian để chương trình thực hiện xóa.

Mục này được chọn thì chương trình sẽ tự động xóa những dữ liệu mà bạn đã chọn trong vòng 1 giờ, kể từ khi bạn bắt đầu khởi động chương trình (xem hình 5.14).



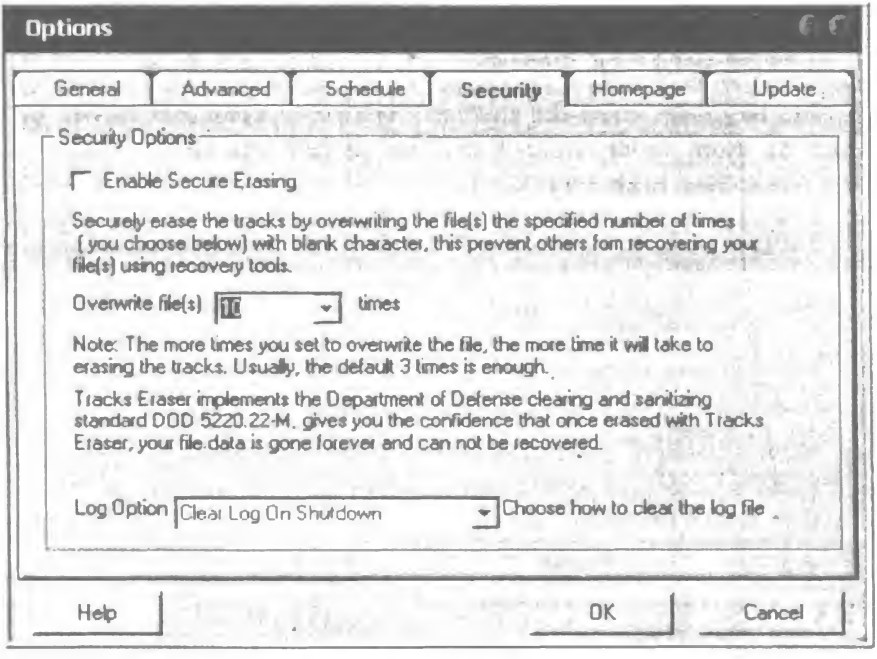
Hình 5.14: *Những thiết lập trong thẻ Schedule.*

1.4. Những thiết lập trong thẻ Security

Mục này cho phép bạn thiết lập tùy chọn liên quan đến quá trình bảo mật khi áp dụng xóa cho các đối tượng dữ liệu. Để thực hiện, bạn làm như sau:

1. Tại hộp thoại Options, nhấp chọn thẻ **Security**.
2. Tại thẻ này, nhấp chọn vào các mục sau:

- **Enable Secure Erasing:** bật tính năng bảo mật khi xóa, tại mục này, nhập vào số lần ghi đè, mặc định là 3. Ví dụ, nhập 10.
- Chọn **Clear log on shutdown** trong mục Log Options, mục này cho phép xóa nội dung tập tin log tại thời điểm shutdown máy tính (xem hình 5.15).



Hình 5.15: *Những thiết lập trong thẻ Security.*

3. Nhấp **OK** để áp dụng các thiết lập.

2. Những thiết lập liên quan đến quá trình xóa dữ liệu

Mục này cho phép bạn thiết lập các mục liên quan đến quá trình xóa dữ liệu trong máy tính của bạn như: xóa Cookies, History, Temporary files,... để thực hiện bạn làm như sau:

2.1. Những thiết lập cho các trình duyệt

Khi thường xuyên truy cập Internet, những thông tin như username và password đã đăng nhập vào các website từ trên các trình duyệt, cũng như URLs đã viếng thăm được lưu lại trong Cookies, History, Internet Temporary files,... Để an toàn và không muốn lưu lại dấu vết nào bạn phải xóa sạch những thông tin trên.

1. Những thiết lập trong thẻ Internet Explorer (IE)

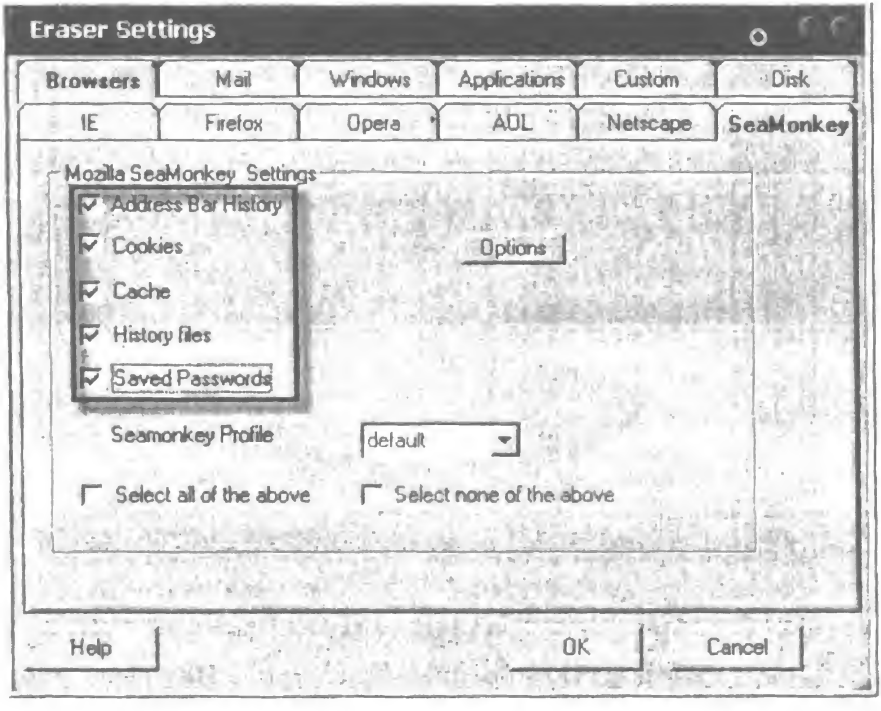
Để thực hiện, bạn làm như sau:

1. Vào **Start > Programs > Tracks Eraser Pro > Tracks Eraser Pro** để mở giao diện chính của chương trình.
2. Tại giao diện chính của chương trình, bạn nhấp chọn thẻ **Eraser Setting > Browse > IE**.

Mục này cho phép bạn thiết lập liên quan đến việc xóa những thông tin mà trình duyệt Internet Explorer lưu lại.

3. Tại thẻ IE bạn nhấp chọn vào các mục sau:

- **Address bar History:** xóa sạch những thông tin lưu lại trên thanh Address của trình duyệt.
- **Cookies:** xóa sạch những thông tin lưu trong Cookies.
- **Cache:** xóa sạch những thông tin trong Cache.
- **History files:** những tập tin được lưu trong History.
- **Saved password:** xóa sạch những password được lưu (xem hình 5.16).



Hình 5.16: *Những thiết lập trong thẻ IE.*

Đối với những trình duyệt khác bạn thực hiện tương tự như trên.

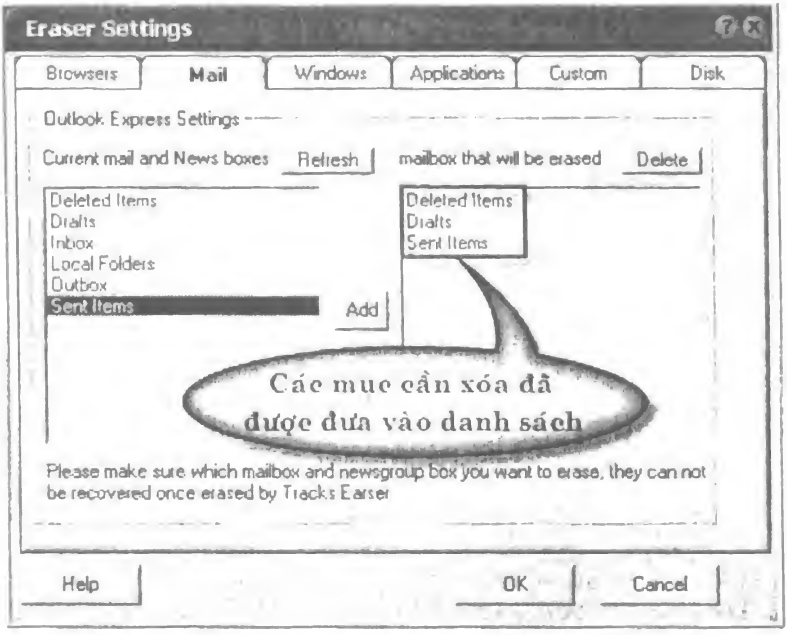
2. Những thiết lập trong thẻ Email

Thẻ này cho phép bạn thiết lập những mục liên quan đến việc xóa sạch những thông tin riêng tư, những dữ liệu nhạy cảm, những thông tin khách hàng, để thực hiện, bạn làm như sau:

1. Vào **Start > Programs > Tracks Eraser Pro > Tracks Eraser Pro** để mở giao diện chính của chương trình.
2. Tại giao diện chính của chương trình, nhấp chọn **Eraser Setting > Mail**
3. Tại thẻ này, bạn đưa các mục sau vào Mailbox that will be erased:

- **Deleted items:** những thư đã xóa.
- **Drafts:** những thư rác.
- **Sent Items:** những thư đã gửi.

Ngoài ra, bạn có thể tham khảo thêm những mục khác mà chương trình gợi ý (xem hình 5.17).



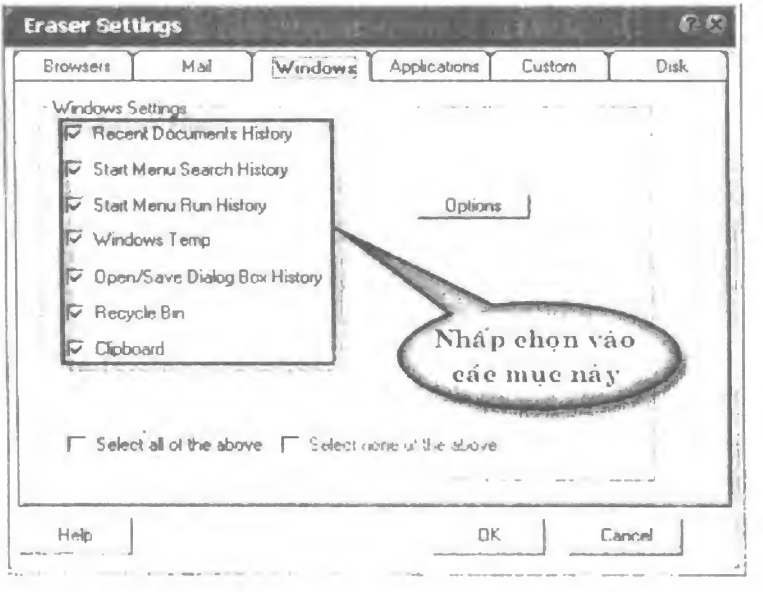
Hình 5.17: *Những thiết lập trong thẻ Mail.*

3. Xóa những thông tin nhạy cảm trong Windows

Những thông tin được lưu lại trong Windows đôi khi cũng rất nguy hiểm, những tài liệu quan trọng mà bạn đã mở cũng được Windows lưu lại trong mục Documents, hay những lệnh mà bạn đã gọi trong menu Run, Tất cả những thông tin trên có thể là nguyên nhân dẫn đến việc máy tính của bạn bị xâm nhập và bị khai thác tài nguyên. Để xóa sạch những thông tin trên, thực hiện như sau:

1. Vào **Start > Programs > Tracks Eraser Pro > Tracks Eraser Pro** để mở chương trình.
2. Tại giao diện chính của chương trình, nhấp chọn **Eraser Setting > Windows**.
3. Tại thẻ này, nhấp chọn vào các mục sau:

- **Recent Document History:** xóa sạch những tài liệu vừa mở được lưu trong mục Recent Document.
- **Start Menu Search History:** xóa sạch những thông tin mà ta đã tìm được lưu trong menu Search.
- **Start Menu Run History:** xóa sạch những thông tin được lưu trong menu Run.
- **Windows Temp:** xóa sạch những dữ liệu trong thư mục Temp của Windows.
- **Open/Save Dialog Box History:** xóa sạch những thông tin được lưu trong hộp thoại Open hoặc Save.
- **Recycle Bin:** xóa sạch những dữ liệu được đưa vào Recycle Bin.
- **Clipboard:** xóa sạch dữ liệu đã đưa vào clipboard (xem hình 5.18).

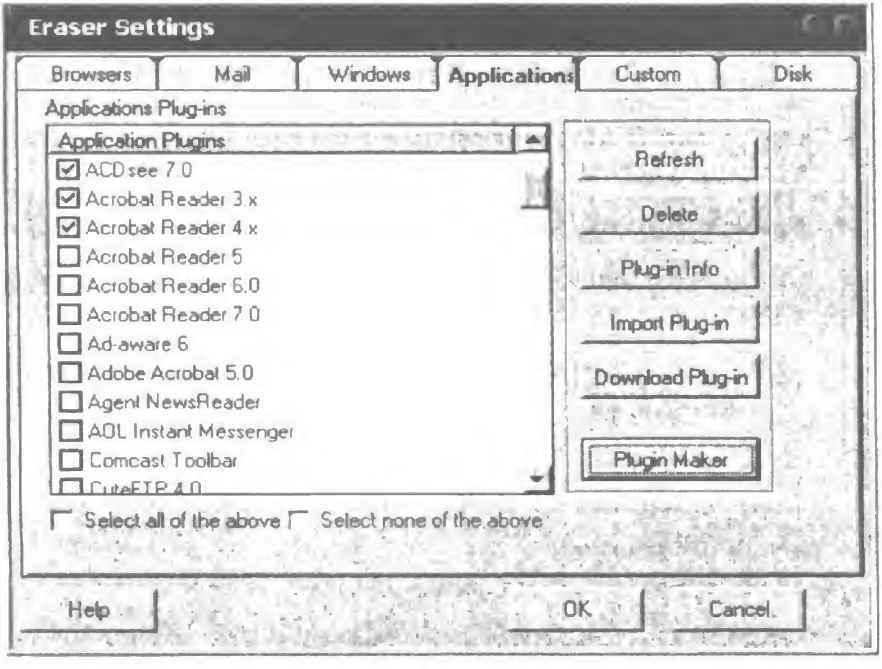


Hình 5.18: *Những thiết lập trong mục Windows*

4. Những thiết lập liên quan đến ứng dụng

Mục này cho phép thiết lập các mục liên quan đến quá trình xóa sạch những thông tin tạm mà các ứng dụng thường tạo ra. Để thực hiện, bạn làm như sau:

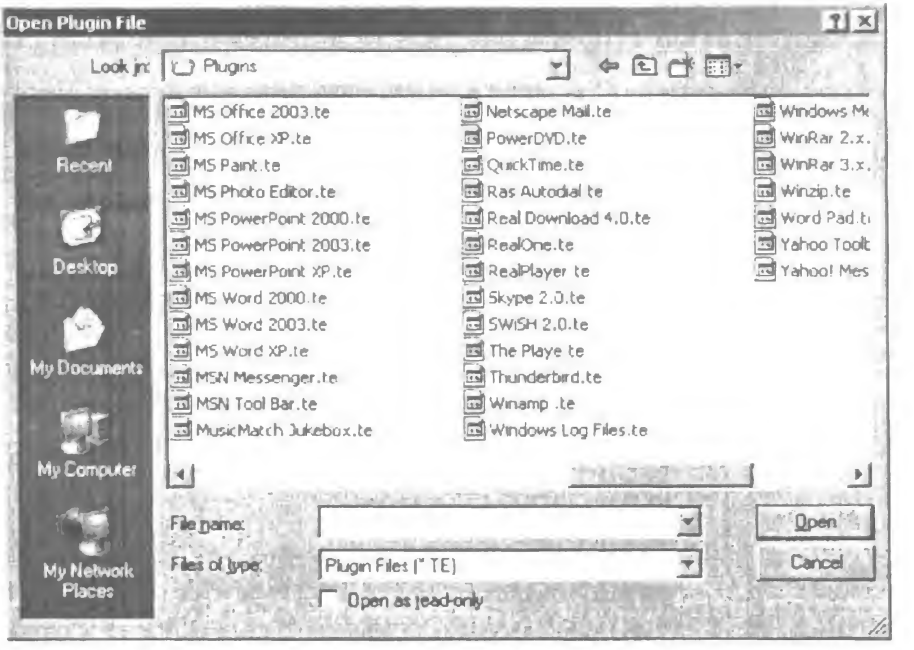
1. Vào **Start > Programs > Tracks Eraser Pro > Tracks Eraser Pro** để mở chương trình.
2. Tại giao diện chính của chương trình, nhấp chọn **Eraser Setting > Applications**.
3. Tại thẻ này, ở mục Applications Plugins, bạn nhấp chọn vào loại ứng dụng mà bạn muốn xóa những thông tin tạm của nó (xem hình 5.19).



Hình 5.19: *Chọn loại ứng dụng muốn xóa.*

4. Nếu những thông tin mà bạn muốn chọn không có trong mục mục Applications Plugins, bạn có thể nhấp nút **Import Plug ins** để đưa những mục mà bạn quan tâm vào danh sách.

Chương trình cung cấp cho chúng ta rất nhiều các Plug – ins được lưu trong thư mục C:\Program files\Acesoft\Tracks Eraser Pro\Plugins (xem hình 5.20).



Hình 5.20: *Danh sách các Plugins.*

5. Nếu những mục mà bạn quan tâm thực sự không có trong danh sách các Plug – ins mà chương trình cung cấp, bạn có thể nhấp nút Download Plug in để download các plugins mới.

6. Bạn cũng có thể tự tạo các Plug–ins bằng cách nhấp nút **Plugins Maker** để tạo ra các plugins riêng.

7. Tiếp theo, nhấp **OK** để áp dụng.

3. Xóa thư mục và tập tin chỉ định

Khi có một thư mục chứa những tài liệu mật hoặc dữ liệu riêng tư, sau khi đã tiến hành sao lưu và cất giữ ở một nơi an toàn, vấn đề còn lại là xử lý thư mục này trên đĩa cứng của máy tính. Bạn không thể xóa nó một cách thông thường được, vì như thế dữ liệu rất có thể phục hồi lại được một cách nhanh chóng. Mục này sẽ giúp xóa sạch những tập tin, thư mục được chỉ định.

1. Vào **Start > Programs > Tracks Eraser Pro > Tracks Eraser Pro** để mở giao diện chính của chương trình.

2. Tại giao diện chính, nhấp nút **File Shredder** để mở hộp thoại Tracks Eraser File Shredder.

3. Tại hộp thoại này, nhấp nút **Options** để mở hộp thoại Options.

4. Nhập vào số lần ghi đè trong mục Overwrite Files, ví dụ 35, tiếp theo nhấp **OK** để áp dụng.

Bạn có thể nhập vào số lần ghi đè tùy ý, tuy nhiên số lần ghi chồng càng nhiều thì khả năng phục hồi dữ liệu càng thấp (xem hình 5.21).

Hình 5.21: *Nhập số lần overwrite.*

5. Tại hộp thoại Tracks Eraser File Shredder, bạn nhấp nút **Select File** để mở tập tin muốn xóa. Sau đó nhấp nút **Start Shredding** để tiến hành xóa.

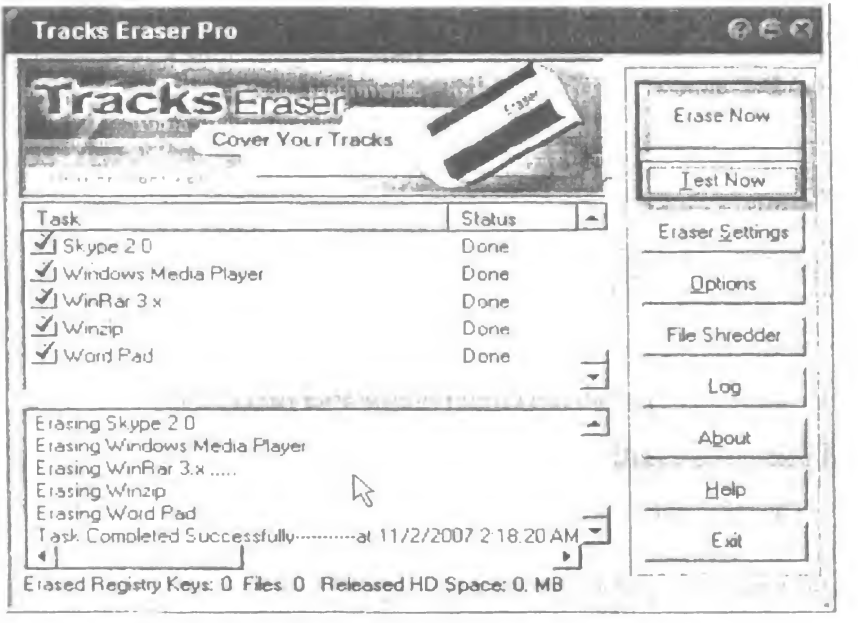
6. Nhấp nút **Select Folder** để mở thư mục bạn muốn xóa, sau đó nhấp nút **Start Shredding** để xóa.

Bạn có thể chọn nhiều thư mục để xóa (xem hình 5.22).

Hình 5.22: *Xóa thư mục.*

4. Xóa nhanh những mục chọn

1. Vào **Start > Programs > Tracks Eraser Pro > Tracks Eraser Pro** để mở chương trình.
2. Ngay trên giao diện chính của chương trình, bạn nhấp nút **Test now** để kiểm tra và thống kê các mục.
3. Nhấp nút **Erase Now** để tiến hành xóa (xem hình 5.23).



Hình 5.23: *Xóa nhanh trên giao diện chính.*

IV. Một số chương trình bảo mật khác

1. R-Wipe and Clean

Đây là giải pháp hoàn chỉnh giúp xóa những tập tin không sử dụng nữa và dữ liệu riêng tư. Nếu những dữ liệu được xóa bằng công cụ này thì không thể phục hồi lại dưới bất kỳ hình thức nào.

Ngoài ra chương trình còn hỗ trợ xóa những thông tin khác như: Temporary files (những tập tin tạm được tạo ra trong quá trình duyệt web), History, URL, ..., và giải phóng không gian đĩa một cách hiệu quả.

2. Directory Snoop

Đây là công cụ tìm kiếm ở mức Cluster, nó cho phép người dùng Windows thực hiện trên tập tin hệ thống FAT hoặc NTFS, và hiển thị tất cả những dữ liệu dưới các track và từ đó bạn có thể xóa hoặc hoặc tìm lại bất kỳ dữ liệu nào mà chương trình hiển thị trong danh sách. Chương trình có những chức năng chính sau:

- Tìm lại những tập tin đã xóa.
- Phá hủy dữ liệu được chỉ định với mức ghi đè trên 35 lần.
- Bảo mật và giải phóng bộ nhớ.
- Lọc những tập tin bị hỏng.
- Tìm và lọc những tên chung.
- Xem, tìm, lọc và sao chép những dữ liệu thô dưới dạng Cluster.
- Liên kết các Cluster động với các chuỗi Cluster mà bạn sử dụng.
- Quét FAT và Master File Tables (MFT).
- Xem các tập tin thông qua những ứng dụng chung.

3. East-Tec Eraser 2007

Chương trình này cho phép bạn dễ dàng xóa những dữ liệu nhạy cảm trên đĩa cứng. Chương trình sử dụng nhiều giải thuật khác nhau để xóa dữ liệu. Một số chức năng chính sau:

- Xóa những dữ liệu riêng tư.
- Xóa những dữ liệu nằm trong Recycle Bin.
- Xóa tập tin và thư mục được chỉ định.
- Tẩy sạch những emails đã xóa.
- Xóa tất cả dữ liệu trong phân vùng được chỉ định.

4. Clean Space Ultimate

Đây là chương trình cho phép bạn nhanh chóng giải phóng không gian đĩa bằng cách xóa những thông tin được tạo ra mặc định từ các ứng dụng, ngoài ra chương trình còn cho phép xóa những thông tin riêng tư bằng phương pháp ghi đè.

Chương trình này tương thích với mọi Windows.

5. Privacy Eraser Pro

Đây là chương trình xóa History và những thông tin khác được lưu lại từ những hoạt động của người dùng trong máy tính. Có thể bạn không thấy rõ được rằng Windows và các chương trình ứng dụng lưu trữ những thông tin về bất kỳ những gì bạn làm, bất kỳ những tài liệu nào mà bạn đã sử dụng, tất cả các website mà bạn đã viếng thăm, những hình ảnh và phim mà bạn đã xem và nhiều hoạt động khác mà bạn đã thực hiện trong máy tính. Nhưng Windows lại không có các chức năng bảo vệ những dấu vết này, hầu hết những thông tin trên đều có thể bị xóa một cách dễ dàng.

Privacy Eraser Pro được thiết kế đặc biệt để loại bỏ những thông tin được hệ thống lưu lại, những dấu vết này thường là những bằng chứng về một hành vi nào đó của bạn trên máy tính.

Chương trình tương thích với mọi Windows.

6. BCWipe 3.0

Hệ thống BCWipe bao gồm tiện ích BCWipe Task Manager, tiện ích này cho phép bạn cấu hình BCWipe để tự động xóa, bạn có thể thiết lập thời gian cho từng nhiệm vụ cụ thể và các tùy chọn cụ thể cho từng nhiệm vụ. Ví dụ, ta cấu hình BCWipe để giải phóng không gian đĩa cho tất cả các phân vùng vào ngày thứ sáu và sử dụng phương pháp US DoD 5200.28-STD để xử lý.

7. Clean Disk Security

Chương trình này có 3 chức năng chính. Thứ nhất nó có thể xóa những dung lượng trống trên đĩa cứng của bạn để đảm bảo rằng các tập tin sẽ không thể phục hồi lại được. Xóa những dung lượng trống trên đĩa cứng hoàn toàn không ảnh hưởng đến những tập tin đang tồn tại.

Thứ hai, chương trình được sử dụng để tẩy sạch những tập tin đang tồn tại, điều này có nghĩa rằng những tập tin được xóa bằng công cụ này sẽ không thể phục hồi lại được.

Thứ ba, chương trình có khả năng giải phóng không gian đĩa bằng cách xóa những tập tin tạm trên đĩa cứng. Ngoài ra chương trình còn có khả năng xóa những dấu vết trong Cookies, History, Internet Temporary File...

Chương trình tương thích với mọi Windows.

8. Secure Clean PC

Những tập tin và thư mục mà chúng ta đã xóa được đưa vào thùng rác (Recycle Bin), và ngay cả khi chúng ta đã xóa chúng trong thùng rác thì Windows cũng chỉ làm một nhiệm vụ là xóa đi liên kết từ tên tập tin cho đến địa chỉ lưu trữ nó. Điều này cũng giống như là ta chỉ xóa đi phần mục lục của một cuốn sách mà chưa hủy phần nội dung.

Chương trình này được thiết kế đặc biệt để giúp bạn giải quyết các vấn đề trên. Bạn có thể download chương trình này tại website www.minhkhai.com.vn, thư mục Chapter 5.

Chương 6:

XÓA DẤU VẾT BẰNG PHƯƠNG PHÁP THỦ CÔNG

- **Một số dấu vết trong máy tính.**
- **Xóa dấu vết mở files.**
- **Xóa dấu vết trong trình duyệt Internet Explorer.**
- **Xóa dấu vết trong trình duyệt Mozilla Firefox.**
- **Xóa dấu vết trong trình duyệt Netscape Navigator.**
- **Xóa dấu vết trong trình duyệt Safari.**
- **Xóa dấu vết trong trình duyệt Flock.**
- **Xóa dấu vết trong trình duyệt Green Browser.**
- **Xóa dấu vết trong trình duyệt Opera.**

Khi đăng nhập vào một hệ thống hoặc một máy tính nào đó thì Windows cũng như những ứng dụng đã sử dụng đều có chức năng ghi lại những hoạt động nhằm theo dõi sở thích, thói quen của bạn.

Trình duyệt thường có các Cookies, History, Temporary Internet Files,... Những thông tin trong những mục trên được lưu trữ trong máy tính, nó chứa những liên kết đến các website mà bạn đã viếng thăm, những thông tin về username và password, tài khoản ngân hàng, hoặc những hình ảnh và phim mà bạn đã xem. Tất cả đều được lưu lại. Cho đến hiện nay thì vẫn chưa có cơ chế và chức năng nào để bảo vệ những thông tin đó. Tất cả những thông tin này đều có thể được xóa dễ dàng.

Để đảm bảo tính bảo mật thì mọi hành vi của bạn trong máy tính đều phải được xóa sạch. Có rất nhiều phần mềm hỗ trợ việc xóa an toàn những thông tin trên và đã được giới thiệu trong chương 5. Tuy nhiên không phải lúc nào bạn cũng có thể sử dụng những phần mềm này.

Chính vì vậy mà trong chương này chúng tôi sẽ giới thiệu đến các bạn một số phương pháp xóa sạch dấu vết bằng phương pháp thủ công.

I. Một số dấu vết trong máy tính

1. Tìm hiểu về Cookies

Cookies là những phần dữ liệu nhỏ có cấu trúc được chia sẻ giữa Web server và trình duyệt (browser) của người dùng. Cookies cung cấp cho server thông tin để nhận biết người dùng, cũng như sở thích, thói quen của họ. Cookies sử dụng các biểu mẫu yêu cầu người dùng điền vào khi họ đến thăm một Web site có hỗ trợ chúng. Không phải mọi trình duyệt đều có thể hỗ trợ Cookies.

Cookies là những tập tin dữ liệu nhỏ, dưới 4 KB. Chúng được các trang World Wide Web tạo ra để truy tìm những người đã ghé thăm website và những vùng mà họ đã đi qua trong website này. Cookies được trình duyệt của người dùng chấp nhận cho lưu trên đĩa cứng của máy tính (máy khách). Trong những phiên truy cập sau, Web server truy cập những thông tin của Cookies, trong đó có tên đăng nhập và password, nên người dùng không phải làm thủ tục đăng nhập mỗi khi họ thăm Web site. Nhưng vấn đề là ở chỗ Web site này có thể dùng thông tin cá nhân của bạn để phục vụ cho mục đích quảng cáo.

Netscape Communications Corp. là hãng đầu tiên sử dụng Cookies trong trình duyệt và ngay sau đó, Microsoft cũng chấp nhận kỹ thuật này. Nhưng không phải trình duyệt nào cũng hỗ trợ Cookies, đặc biệt là những phiên bản cũ.

Rõ ràng Cookies chứa đựng trong nó những nguy cơ về bảo mật. Ví dụ, hacker có thể lấy tài khoản ngân hàng của người dùng thông qua việc chỉnh sửa Cookies. Sau đó, anh ta có thể sử dụng dữ liệu này để truy cập tài khoản của người dùng một cách hợp pháp.

Những trình duyệt mới hơn cho phép người dùng khóa các Cookies hoặc xin phép họ trước khi lưu lại Cookies trên hệ thống. Một số phần mềm của các hãng thứ ba cũng giúp quản lý Cookies. Nhưng đối với người dùng, thật khó biết tại sao Cookies lại có mặt trên hệ thống của họ cũng như những Cookies này chứa đựng thông tin gì.

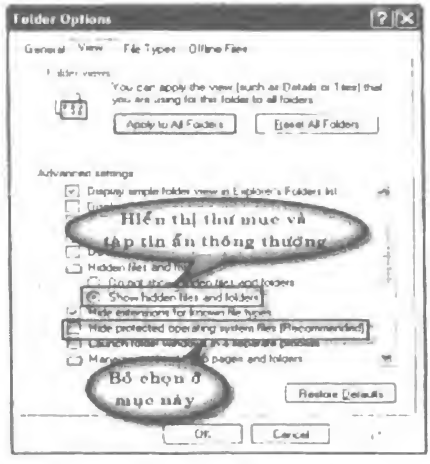
2. Vị trí lưu trữ của Cookies

Trong Windows, thư mục lưu trữ Cookies được ẩn ở dạng đặc biệt, để nhìn thấy thư mục này bạn phải cho hiện những tập tin và thư mục ẩn trong máy tính. Phương pháp thực hiện như sau:

1. Nhấp phải chuột vào biểu tượng của **My Computer** trên Desktop, chọn **Explorer** để mở cửa sổ My Computer dưới dạng Explorer.

2. Tại cửa sổ My Computer, vào menu **Tools > Folder Options** để mở hộp thoại Folder Options.

3. Chọn thẻ **View**, tiếp theo nhấp chọn vào mục **Show hiden files and folders** và bỏ chọn ở mục **Hide protected operating system files (recommended)** (xem hình 6.1).



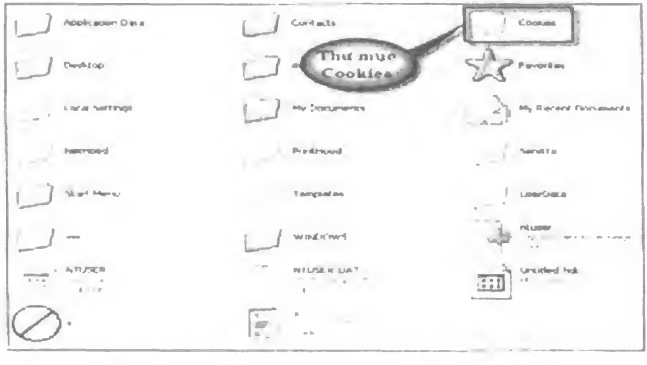
Hình 6.1: *Hiển thị tập tin và thư mục ẩn.*

4. Tiếp theo, nhấp **OK** để áp dụng.

Lúc này tất cả những tập tin và thư mục ẩn (cả những thông tin được ẩn đặc biệt) trong máy tính đều được hiển thị.

5. Tại cửa sổ My Computer, bạn nhấp chọn vào ổ đĩa **C**, tiếp theo chọn **Documents and Settings > Security**.

Trong đó Security là tài khoản mà user đăng nhập vào máy tính (xem hình 6.2).



Hình 6.2: *Vị trí thư mục Cookies.*

3. Tìm hiểu về Temporary Internet Files

Đây là những tập tin được tạo ra khi viếng thăm một website nào đó, những hình ảnh, những liên kết được nạp vào máy tính để trình duyệt có thể chạy website nhanh hơn. Tuy nhiên nếu số lượng website viếng thăm quá nhiều thì dung lượng của các tập tin này trên đĩa cứng cũng không phải là nhỏ.

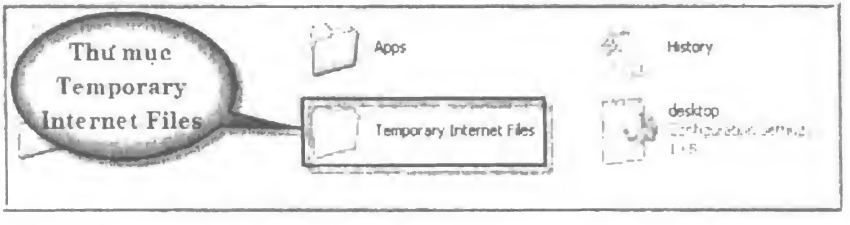
Hơn nữa một số tập tin còn có thể chứa những mã nguồn nguy hiểm của virus, trojan, worm. Để đảm bảo tính bảo mật cũng như giải phóng không gian đĩa thì những tập tin này phải được xóa sạch trong máy tính.

4. Vị trí lưu trữ của Temporary Internet Files trong máy tính

Những tập tin này còn được gọi là Cache files. Thư mục chứa các tập tin này luôn tồn tại trong máy tính ở dạng ẩn đặc biệt. Muốn hiển thị thư mục chứa những tập tin này bạn phải thực hiện từ bước 1 đến 4 như ở phần trên. Để tìm vị trí lưu trữ các tập tin này bạn thực hiện như sau:

1. Nhấp phải chuột vào biểu tượng của **My Computer** trên Desktop, chọn **Explorer** để mở cửa sổ My Computer dưới dạng Explorer.
2. Tại ô bên trái, nhấp chọn vào ổ đĩa C, tiếp theo chọn **Documents and Settings > Security > Local Settings > Temporary Internet Files**.

Trong đó Security là tài khoản của User đăng nhập vào máy tính (xem hình 6.3).



Hình 6.3: *Thư mục Temporary Internet Files.*

5. Tìm hiểu về History

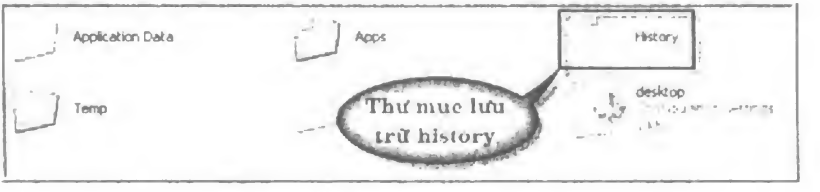
Mỗi khi duyệt web đều được các trình duyệt lưu lại các hoạt động của bạn như: website đã viếng thăm, URLs đã nhập vào vào thanh address của trình duyệt. Tất cả đều được trình duyệt ghi lại và lưu trữ trong một nơi gọi là History. Để tìm hiểu sâu hơn về History, bạn thực hiện như sau:

6. Vị trí lưu trữ của History

Để biết vị trí lưu trữ của History trong máy tính bạn thực hiện như sau:

1. Nhấp phải chuột vào biểu tượng của **My Computer** trên Desktop, chọn **Explorer** để mở cửa sổ My Computer dưới dạng Explorer.
2. Tại ô bên trái, nhấp chọn vào ổ đĩa **C > Documents and Settings > security > Local Settings > History**.

Trong đó, security là tên tài khoản mà người dùng đăng nhập vào máy tính, History là thư mục được ẩn dưới dạng đặc biệt trong máy tính, muốn hiển thị thì bạn phải thực hiện từ bước 1 đến 4 của mục "**Vị trí lưu trữ của Cookies**" (xem hình 6.4).



Hình 6.4: *Vị trí của History.*

7. Tìm hiểu về những tập tin Temporary

Temporary là những tập tin được sử dụng tạm thời do những chương trình tự sinh ra trong quá trình thực hiện hoặc khi cài đặt.

Thư mục chứa những tập tin Temporary này có tên là Temp. Nếu những tập tin trong thư mục này lâu ngày không được xóa thì dung lượng sẽ tăng lên đáng kể.

Bản thân những tập tin này thường không chứa virus hay trojan, nhưng nếu như hacker lợi dụng những điểm này để cài đặt virus hoặc trojan thì cũng rất nguy hiểm. Để đảm bảo an toàn và giải phóng dung lượng đĩa cứng bạn phải xóa sạch những thông tin trong thư mục này.

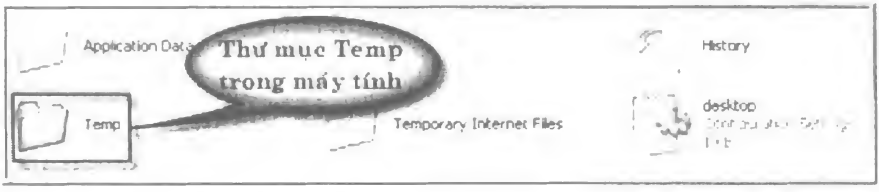
8. Vị trí lưu trữ của Temporary

Để biết được vị trí lưu trữ của thư mục Temporary trong máy tính bạn thực hiện như sau:

1. Nhấp phải chuột vào biểu tượng của **My Computer** trên Desktop, chọn **Explorer** để mở cửa sổ My Computer dưới dạng Explorer.

2. Tại ô bên trái, nhấp chọn vào ổ đĩa **C > Documents and Settings > security > Local Settings**.

Trong đó security là tên tài khoản mà người dùng đăng nhập vào máy tính (xem hình 6.5).



Hình 6.5: *Thư mục Temp của máy tính.*

9. Những tập tin mới mở

Hệ điều hành có chức năng lưu trữ những tập tin mới mở, đây là một chức năng hay, nhưng nhiều khi cũng gây ra nhiều rắc rối. Vì nó sẽ vô tình là những bằng chứng nói lên một điều, bạn là người mới truy cập vào một tập tin nào đó trong máy tính hệ thống hoặc hệ thống.

Những thông tin này thường được hiển thị trong **Start > Documents** và nhiều mục khác liên quan đến từng chức năng mà nó quản lý.

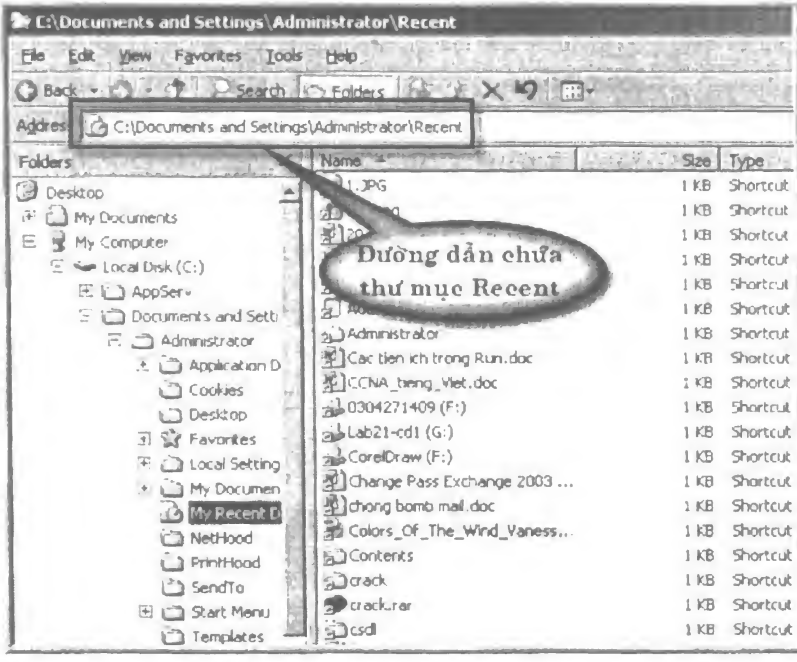
Để xóa bỏ hoàn toàn dấu vết thì những thông tin này phải được loại bỏ khỏi máy tính. Nhưng trước tiên, chúng ta phải tìm hiểu về vị trí lưu trữ của những thông tin này.

Vị trí lưu trữ của thư mục Recent

Để biết được vị trí lưu trữ của thư mục này trong máy tính, bạn thực hiện như sau:

1. Nhấp phải chuột vào biểu tượng của **My Computer** trên Desktop, chọn **Explorer** để mở cửa sổ My Computer dưới dạng Explorer.
2. Ngay trên thanh **Address** của cửa sổ My Computer, bạn nhập **C:\Documents and Settings\security\Recent**.

Trong đó Security là tên tài khoản mà người dùng đăng nhập vào máy tính (xem hình 6.6).



Hình 6.6: *Đường dẫn chứa thư mục Recent.*

10. Loại bỏ dấu vết trong Registry của Windows

Registry của Windows là một cơ sở dữ liệu lớn, nó lưu trữ hầu như là mọi thông tin trong máy tính như: quản lý danh mục phần mềm, các đăng ký trong Windows và lưu trữ đường dẫn của những hình ảnh, video mà bạn đã xem, những website mà bạn đã viếng thăm,...

Để an toàn thì những thông mà bạn đã thực hiện phải đảm bảo xóa sạch trong Registry.

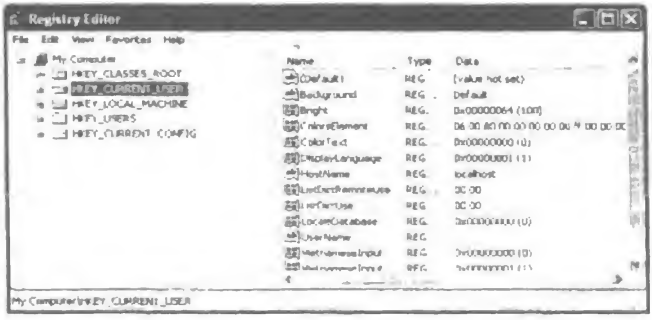
11. Loại bỏ một số thông tin trong Registry

Để đảm bảo an toàn và xóa sạch dấu vết truy cập trong máy tính thì phải loại bỏ những thông tin trong Registry.

11.1. Loại bỏ những tập tin MS Word đã mở

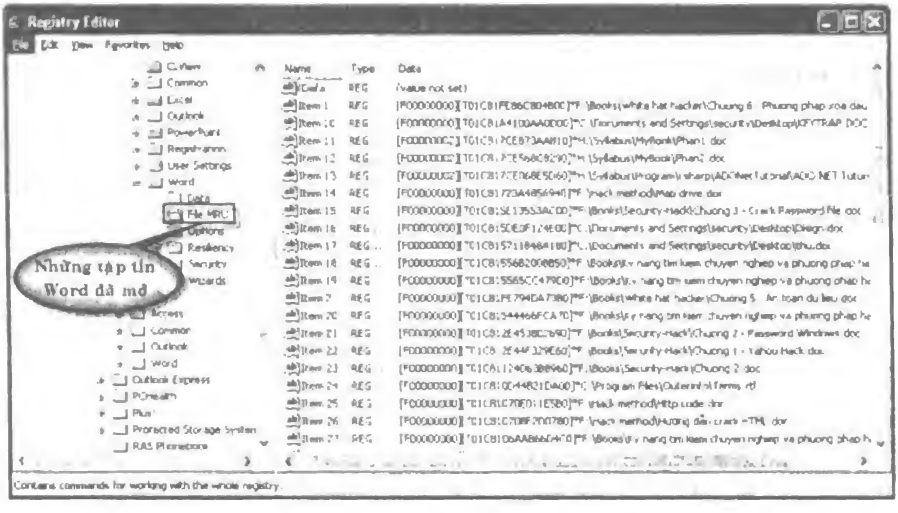
Mỗi khi mở một tập tin của MS Word trong máy tính, thì ngay lập tức những thông tin này được lưu ngay trong Registry, để xóa những thông tin này, bạn thực hiện như sau:

1. Vào **Start > Run** nhập **regedit**, sau đó nhấp **OK** để mở cửa sổ Registry Editor (xem hình 6.7).



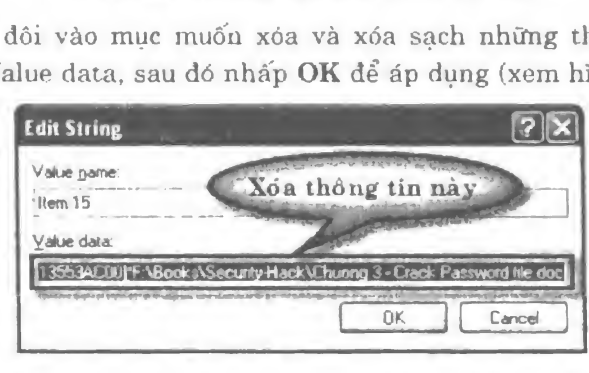
Hình 6.7: *Cửa sổ Registry Editor.*

2. Tại ô bên trái, nhấp chọn vào mục **HKEY_CURRENT_USER > Software > Microsoft > Office > 12.0 > Word > File MRU** (xem hình 6.8).



Hình 6.8: *Những tập tin Word đã mở.*

3. Nhấp đôi vào mục muốn xóa và xóa sạch những thông tin trong mục Value data, sau đó nhấp **OK** để áp dụng (xem hình 6.9).



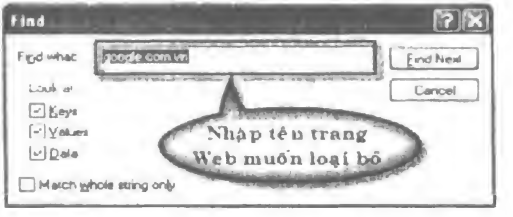
Hình 6.9: *Xóa dấu vết của file word đã mở trong Registry.*

Bạn áp dụng cách tương tự để loại bỏ những dấu vết trong việc mở những files của MS Excel, PowerPoint, Access...

11.2. Loại bỏ những URLs đã nhập trong Registry

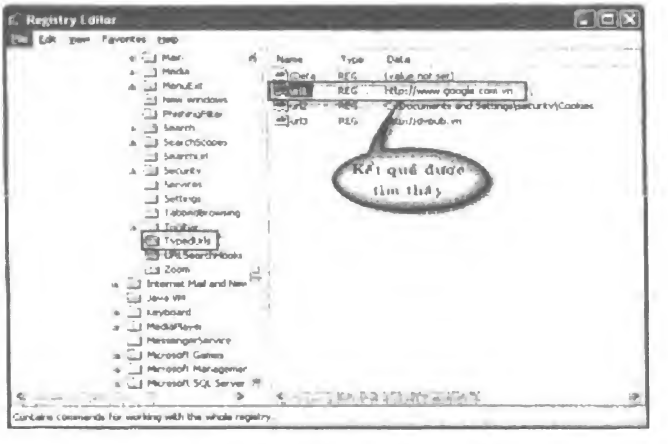
Để loại bỏ những URLs đã nhập trong Registry bạn thực hiện như sau:

1. Vào **Start > Run** nhập **regedit**, sau đó nhấp **OK** để mở cửa sổ Registry Editor.
2. Vào menu **Edit > Find** hoặc nhấn tổ hợp phím **Ctrl + F** để mở hộp thoại **Find**, tiếp theo trong mục **Find what** bạn nhập vào tên trang Web muốn xóa, sau đó nhấp **OK** để tìm, ví dụ nhập **google.com.vn** (xem hình 6.10).

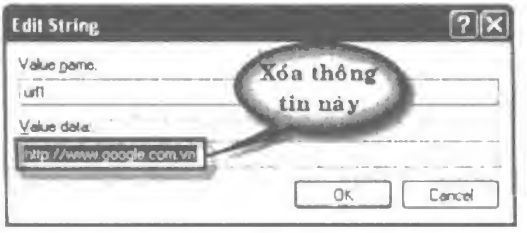


Hình 6.10: *Hộp thoại Find.*

3. Sau khi tìm kiếm xong, chương trình sẽ hiển thị kết quả được tìm thấy trong cửa sổ bên phải (xem hình 6.11).
4. Nhấp đôi vào khóa muốn xóa, sau đó xóa sạch những thông tin trong mục **Value data**. Ví dụ chúng ta sẽ nhấp đôi vào khóa url1, sau đó sẽ xóa sạch những thông tin trong mục Value data (xem hình 6.12).



Hình 6.11: *Kết quả tìm kiếm.*



Hình 6.12: *Xóa những thông tin trong mục Value data.*

Áp dụng cách tương tự để loại bỏ những thông tin khác trong Registry. Những thông tin mà bạn muốn tìm không chỉ nằm ở một nơi, điều này có nghĩa là, sau khi xóa hết những thông tin từ khóa này bạn phải tiếp tục tìm kiếm cho đến khi không còn khóa nào được tìm thấy.

Nếu thực hành những điều này trên máy tính của bạn thì trước tiên, phải sao lưu Registry.

II. Xóa dấu vết mở tập tin

Mỗi một hoạt động của bạn trong máy tinh đều được hệ điều hành cùng một số chương trình khác ghi lại, để xóa các dấu vết này, bạn thực hiện như sau:

1. Xóa những thông tin trong thư mục Recent

Những dấu vết mở tập tin, những lệnh đã thực hiện được nhập trong menu Run,... đều được Windows lưu lại, để xóa những mục này, bạn thực hiện như sau:

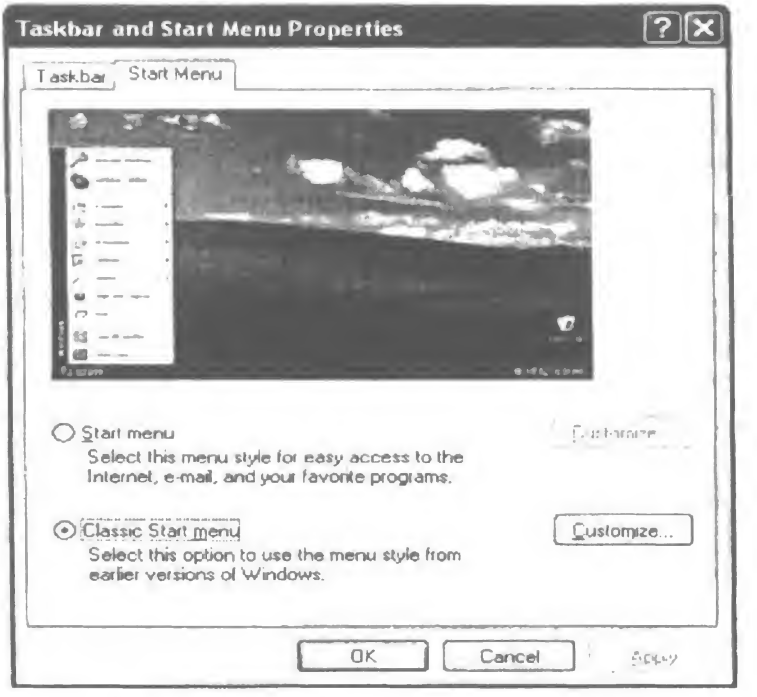
1. Nhấp phải chuột lên thanh **Taskbar**, chọn **Properties**, tiếp theo chọn thẻ **Start menu**.

Hộp thoại Taskbar and Start menu Properties xuất hiện (xem hình 6.13).

2. Nhấp nút **Customnize**, hộp thoại Customize Classis Start Menu xuất hiện, nhấp nút **Clear** để thực hiện (xem hình 6.14).

3. Tiếp theo, nhấp nút **OK** để áp dụng.

Lúc này mọi tập tin xuất hiện trong mục Ducuments và những lệnh đã thực hiện trong menu Run đã được xóa sạch.



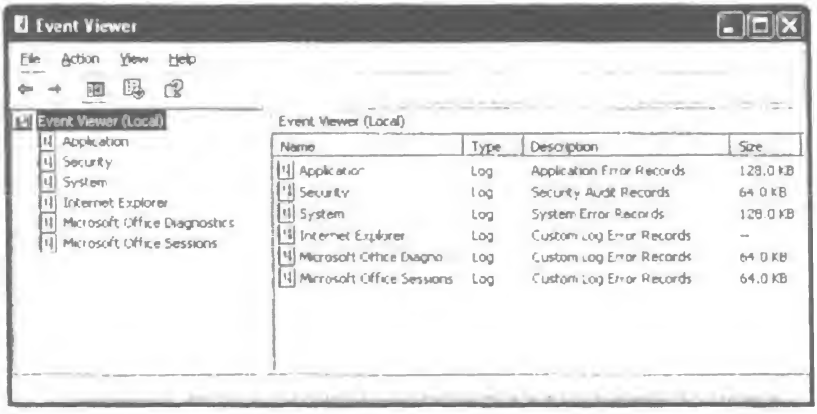
Hình 6.13: *Hộp thoại Taskbar and Start menu Properties.*

Hình 6.14: *Hộp thoại Customize Classis Start Menu.*

2. Xóa những thông tin trong Event Viewer

Event Viewer là chương trình quản lý tập tin log, nó ghi lại những sự kiện của hệ thống và ứng dụng. Để xóa những nhật ký này, bạn thực hiện như sau:

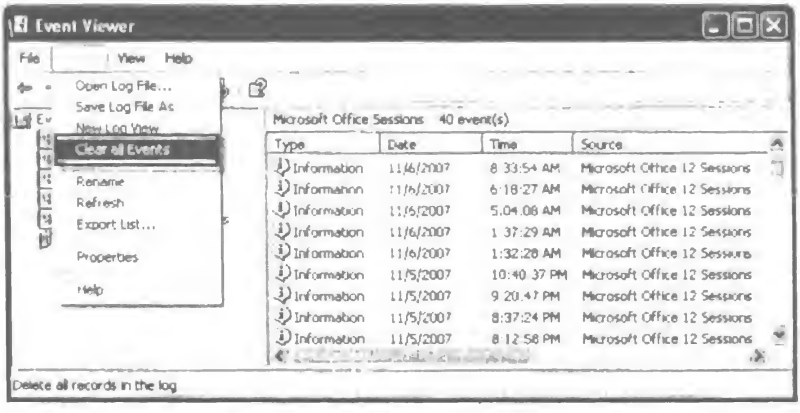
1. Vào **Start > Settings > Control Panel > Administrative Tools** để mở danh mục các công cụ.
2. Nhấp vào mục **Event Viewer** để mở cửa sổ **Event Viewer** (xem hình 6.15).



Hình 6.15: *Cửa sổ Event Viewer.*

3. Tại ô bên trái, nhấp vào loại sự kiện mà bạn muốn xóa thông tin log, sau đó vào menu **Action > Clear all Events** (xem hình 6.16).

Tiếp theo chương trình xuất hiện hộp thoại yêu cầu lưu thông tin, bạn chọn **No** để thực hiện.



Hình 6.16: *Xóa những thông tin trong Event Viewer.*

III. Xóa dấu vết trong trình duyệt Internet Explorer

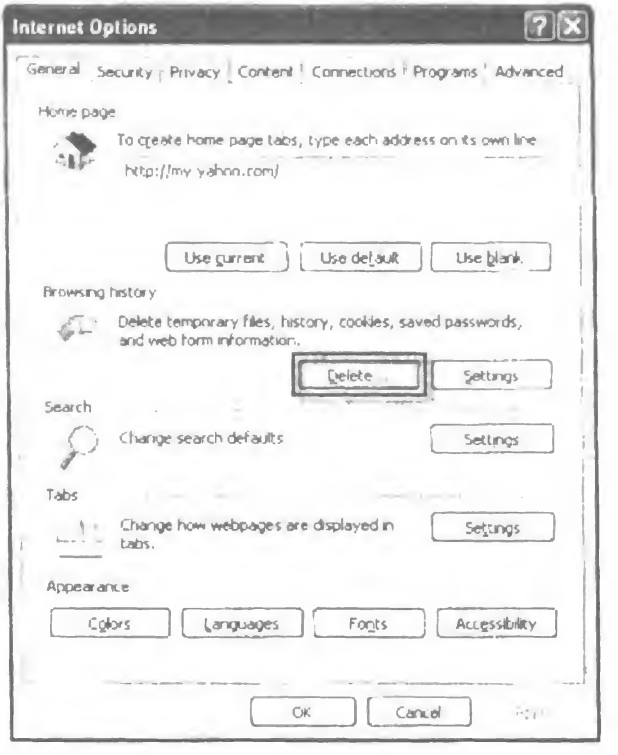
Hầu hết các trình duyệt thông dụng hiện nay đều hỗ trợ Cookies và History, tuy nhiên cũng chưa có trình duyệt nào có chế độ bảo vệ những thông tin mà nó thu được. Chính vì vậy việc loại bỏ những dấu vết từ các trình duyệt là rất đơn giản.

Trong mục này chúng tôi sẽ giới thiệu về trình duyệt Internet Explorer 7.0.

1. Xóa Cookies

Để xóa Cookies đối với trình duyệt Internet Explorer, bạn thực hiện như sau:

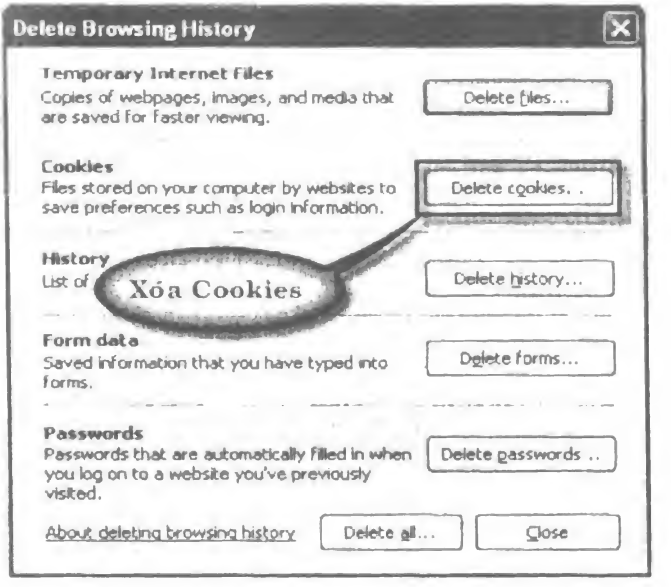
1. Vào **Start > Programs > Internet Explorer** để mở trình duyệt hoặc bạn có thể mở trình duyệt ngay trên Desktop.
2. Trên giao diện của trình duyệt, vào menu **Tools > Internet Opions** để mở hộp thoại Internet Options (xem hình 6.17).



Hình 6.17: *Hộp thoại Internet Options.*

3. Tại hộp thoại Internet Options, bạn nhấp nút **Delete** để mở hộp thoại Delete Brower History. Tiếp theo, tại mục Cookies, nhấp nút **Delete Cookies** để xóa.

Sau khi nhấp nút Delete, chương trình yêu cầu xác nhận thông tin, nhấp **Yes** để thực hiện. Bạn cũng có thể xóa những thông tin khác như: Temporary Internet files, History, Form data, Password từ hộp thoại này (xem hình 6.18)



Hình 6.18: *Xóa Cookies.*

2. Xóa History

1. Vào **Start > Programs > Internet Explorer** để mở trình duyệt hoặc bạn có thể mở ngay trình duyệt này trên Desktop.

2. Tại cửa sổ trình duyệt, nhấn tổ hợp phím **Ctrl + H** để mở cửa sổ History.

Sau khi nhấn tổ hợp phím Ctrl + H, một cửa sổ nhỏ hiển thị và được tích hợp vào bên trái của cửa sổ trình duyệt. Những trang mà bạn đã viếng thăm được hiển trong cửa sổ này. Các liên kết này được sắp xếp theo ngày, tuần, và tháng (xem hình 6.19).

3. Tiếp theo, nhấp phải chuột vào liên kết muốn xóa, sau đó chọn **Delete**.

Sau khi chọn Delete, chương trình yêu cầu bạn xác nhận lại thông tin, nếu đồng ý xóa, bạn chọn **Yes** để thực hiện. Danh sách History được tổ chức thành từng nhóm. Mỗi nhóm tương ứng với thời gian (tính bằng ngày) mà bạn viếng thăm.

Hướng dẫn thêm:

Bạn có thể truy cập History bằng cách nhấp vào nút có biểu tượng hình ngôi sao ở bên góc trái của màn hình, dưới menu File của trình duyệt.

Hình 6.19: *History của trình duyệt Internet Explorer.*

IV. Xóa dấu vết trong trình duyệt Mozilla Firefox

Mozilla Firefox là trình duyệt lớn, hiện nay trên thế giới nó chiếm khoảng 8,6 thị phần, đây là trình duyệt được giới chuyên môn đánh giá rất cao. Và tất nhiên là trình duyệt này cũng hỗ trợ Cookies và nhiều thông tin theo dõi khác. Những thông tin này một mặt cũng hỗ trợ rất tốt đối với người dùng, nhưng mặt khác cũng tạo ra nhiều vấn đề rắc rối nếu ta không biết quản lý nó.

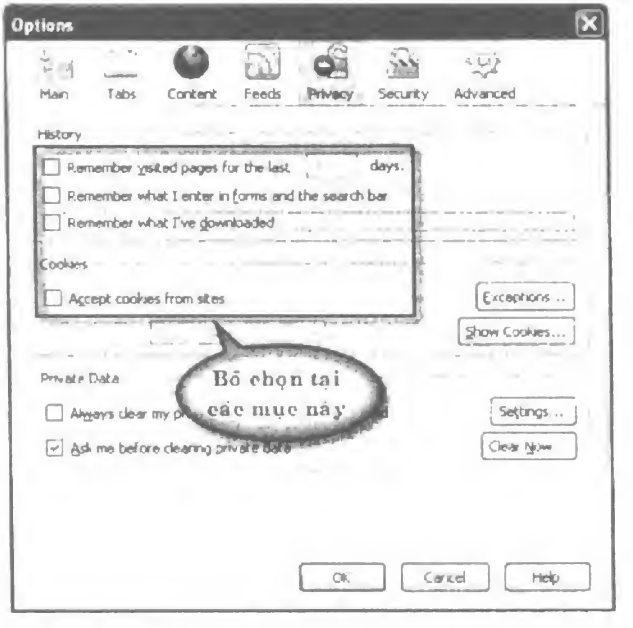
Trong mục này giới thiệu đến các bạn phương pháp xóa dấu vết trên trình duyệt Mozilla Firefox 3.0, đây là phiên bản mới nhất có tên là Minefield.

1. Xóa Cookies

Để xóa Cookies trên trình duyệt Minefied, bạn thực hiện như sau:

1. Vào **Start > Programs > Minefield > Minefield** để mở trình duyệt.
2. Tại cửa sổ trình duyệt, vào menu **Tools > Options** để mở hộp thoại Options, sau đó nhấp chọn vào thẻ **Privacy**. Tại thẻ này, bạn bỏ chọn ở các mục sau:

- **Remember visited page for the last:** nhớ trang đã viếng thăm trong vòng (số ngày).
- **Remember what I enter the forms and the search bar:** nhớ những gì mà bạn đã nhập vào trong form và thanh tìm kiếm.
- **Remember what I've downloaded:** nhớ những gì mà bạn đã Download.
- **Accept Cookies from sites:** truy cập Cookies từ các trang (xem hình 6.20).

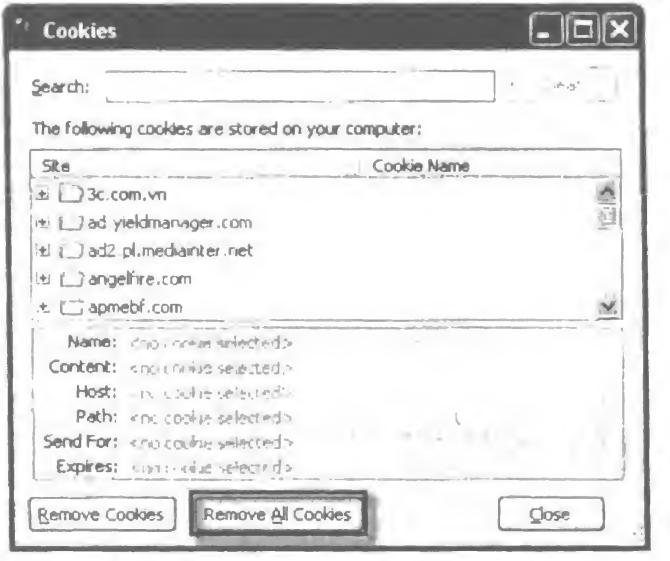


Hình 6.20: *Những thiết lập trong thẻ Privacy.*

3. Nhấp nút **Show Cookies** để mở hộp thoại Cookies, tiếp theo, nhấp nút **Remove All Cookies** (xem hình 6.21).

Bạn cũng có thể nhấp nút Clear Now để xóa Cookies ngay tại hộp thoại Options trong thẻ Privacy.

Như vậy tới đây ta đã hoàn toàn loại bỏ được Cookies trong trình duyệt Mozilla Minefield.



Hình 6.21: *Loại bỏ Cookies trong trình duyệt Minefield.*

2. Loại bỏ History

1. Vào **Start > Programs > Minefield > Minefield** để mở trình duyệt.

2. Tại cửa sổ trình duyệt, nhấn tổ hợp phím **Ctrl + H** để mở cửa sổ History.

Sau khi nhấn tổ hợp phím Ctrl + H, một cửa sổ nhỏ được tích hợp vào phía bên trái của trình duyệt, hiển thị danh sách các liên kết đến các Websites mà bạn đã viếng thăm.

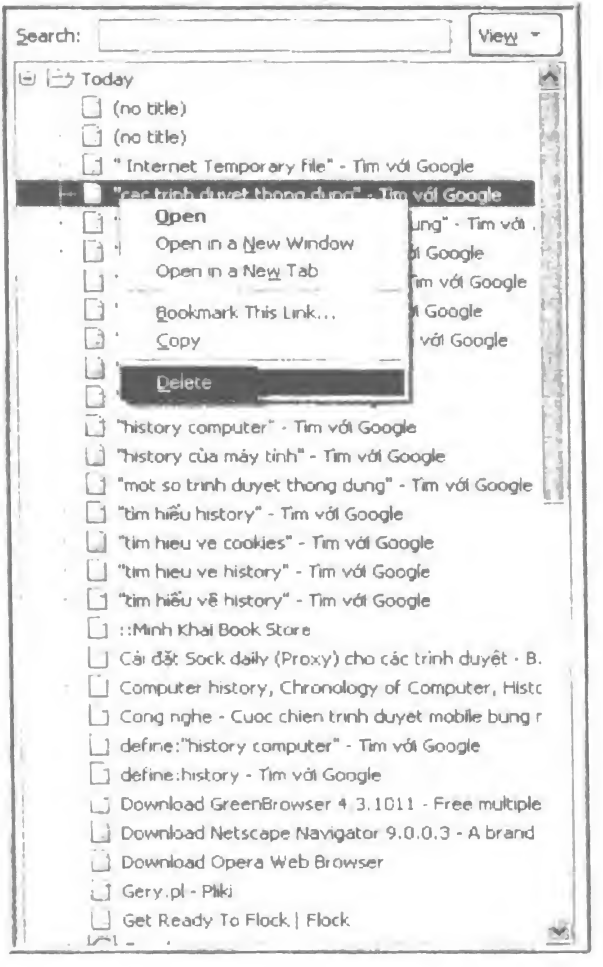
3. Nhấp phải chuột vào liên kết muốn xóa, tiếp theo chọn **Delete** (xem hình 6.22).

Hướng dẫn thêm:

Bạn có thể xem những thông tin History ngay ở giao diện chính của chương trình. Để thực hiện, vào menu History. Tuy nhiên, mục này chỉ cho

phép xem thông tin được ghi lại, nó không cho phép thao tác trên nó. Tức là bạn không thể copy, edit, hay delete được History trong menu này.

Bạn chỉ nên xóa những History cần thiết, điều này có nghĩa là, chỉ nên xóa những dấu vết mà bạn tạo ra. Không nên xóa những mục khác, vì như vậy sẽ vô tình tạo thêm dấu vết mới.



Hình 6.22: *Xóa dấu vết trong History.*

V. Xóa dấu vết trong trình duyệt Netscape Navigator

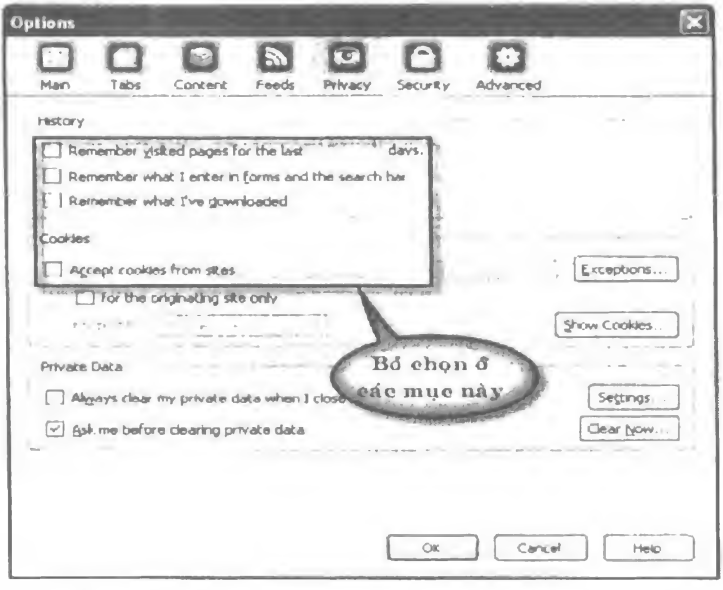
Đây là trình duyệt lớn, đã có tương đối sớm và là trình duyệt đầu tiên sử dụng Cookies. Mục này giới thiệu đến bạn các phương pháp xóa dấu vết trên trình duyệt Netscapse Navigator 9.0.0.3. Đây là phiên bản mới nhất.

1. Xóa Cookies

Cũng tương tự như các trình duyệt khác, để xóa Cookies và loại bỏ các thông tin trong thẻ Privacy, bạn thực hiện như sau:

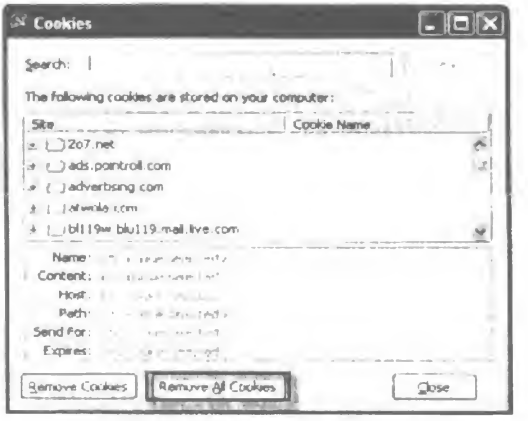
1. Vào **Start > Programs > Netscape Navigator > Netscape Navigator** để mở trình duyệt.
2. Tại cửa sổ trình duyệt, vào menu **Tools > Options** để mở hộp thoại Options, sau đó nhấp chọn vào thẻ **Privacy**. Tại thẻ này, bạn bỏ chọn ở các mục sau:

- **Remember visited page for the last:** nhớ trang đã viếng thăm trong vòng (số ngày).
- **Remember what I enter the forms and the search bar:** nhớ những gì mà tôi đã nhập vào trong form và thanh tìm kiếm.
- **Remember what I've downloaded:** nhớ những gì mà tôi đã Download.
- **Accept Cookies from sites:** truy cập Cookies từ các trang (xem hình 6.23).



Hình 6.23: *Những thiết lập trong thẻ Privacy.*

3. Nhấp nút **Show Cookies**, để mở hộp thoại Cookies, tiếp theo nhấp nút **Remove All Cookies** để loại bỏ tất cả các Cookies được lưu (xem hình 6.24).



Hình 6.24: *Loại bỏ Cookies khỏi Netscape Navigator*

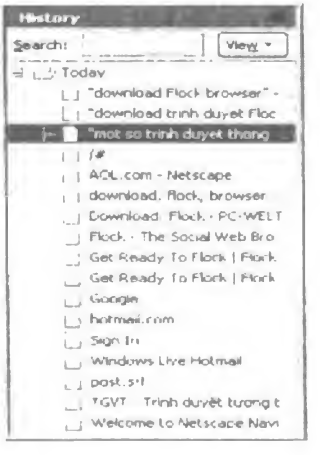
2. Xóa History

Để loại bỏ History khỏi trình duyệt Netscape Navigator, bạn thực hiện như sau:

1. Vào **Start > Programs > Netscape Navigator > Netscape Navigator** để mở trình duyệt.
2. Tại cửa sổ trình duyệt, bạn nhấn tổ hợp phím **Ctrl + H** để mở cửa sổ History.

Sau khi bạn nhấn tổ hợp phim Ctrl + H, chương trình hiển thị một cửa sổ nhỏ được tích hợp ngay bên trái của trình duyệt.

3. Nhấp phải chuột vào liên kết mà bạn muốn xóa, sau đó chọn **Delete** để xóa (xem hình 6.25).



Hình 6.25: *Xóa History của Netscape Navigator.*

VI. Xóa dấu vết trong trình duyệt Safari

Safari là trình duyệt Web của công ty Apple, là trình duyệt tương đối mạnh. Hiện nay, Apple cung cấp trình duyệt này với phiên bản mới nhất là 3.0.3 (522.15.5). Safari được các chuyên gia đánh giá là trình duyệt mạnh, khả năng lướt web nhanh hơn cả Internet Explorer và Mozila Firefox. Đây là trình duyệt được Apple cung cấp cho hệ điều hành Macintosh. Vì là trình duyệt mạnh nên nó cũng hỗ trợ Cookies. Mục này giới thiệu đến bạn phương pháp loại bỏ Cookies và History từ Safari.

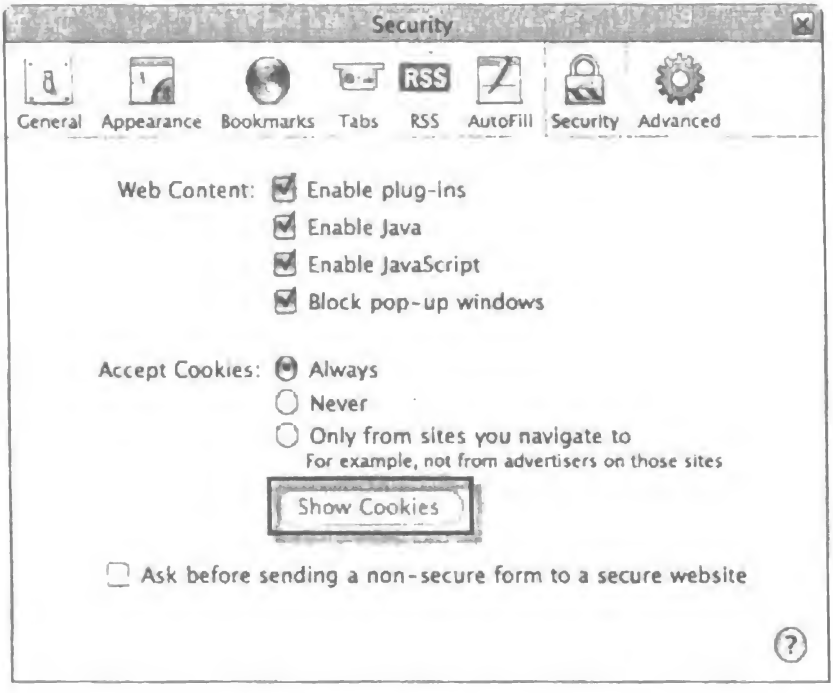
1. Loại bỏ Cookies

Để loại bỏ Cookies trong trình duyệt Safari, bạn thực hiện như sau:

1. Vào **Start > Programs > Safari** để mở trình duyệt.
2. Tại giao diện chính của trình duyệt. Vào menu **Edit > Preferences** hoặc nhấn tổ hợp phím **Ctrl + ,** (nhấn giữ phím Ctrl, nhấn tiếp phím dấu cộng (+) và phím dấu phẩy (,)) để mở hộp thoại General (xem hình 6.26).

Hình 6.26: *Hộp thoại General của trình duyệt Safari.*

3. Tại hộp thoại General, nhấp chọn thẻ **Security**, tiếp theo, bạn nhấp vào nút **Show Cookies** để hiển thị hộp thoại Cookies (xem hình 6.27).



Hình 6.27: *Hiển thị Cookies.*

4. Tại hộp thoại Cookies, nhấp nút **Remove All** để loại bỏ tất cả Cookies.

5. Khi kết thúc bạn nhấp nút **Done** để hoàn thành.

Bạn có thể nhập vào những thông tin cần tìm trong mục Search, sau đó nhấp nút Remove để loại bỏ đi những Cookies thực sự cần thiết. Những mục khác không liên quan bạn nên để lại.

2. Xóa History

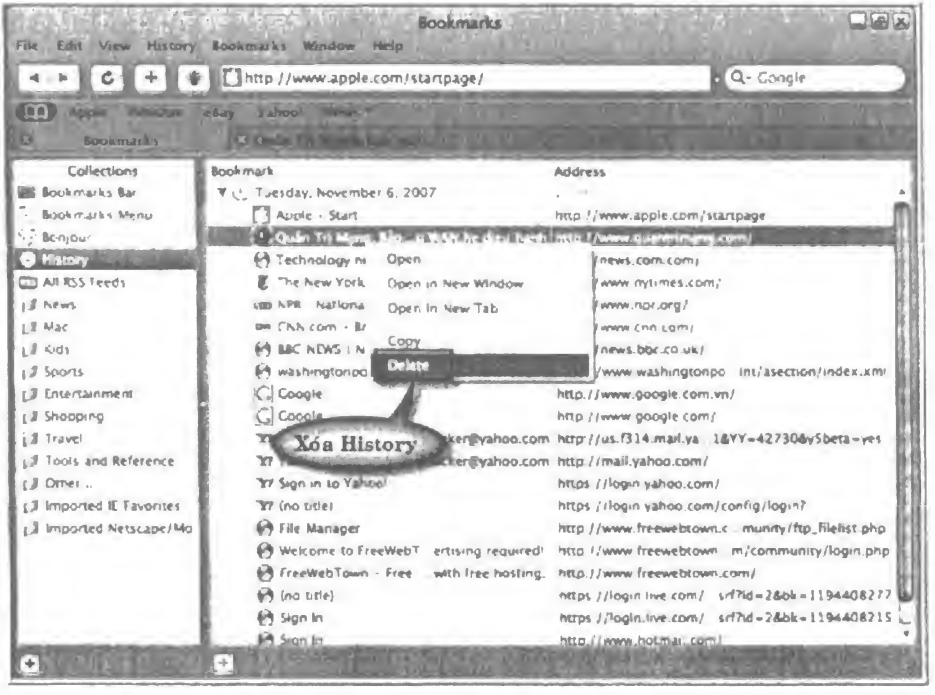
Để loại bỏ History trong trình duyệt Safari bạn thực hiện như sau:

1. Vào **Start > Programs > Safari** để mở trình duyệt.

2. Tại giao diện chính của trình duyệt, vào menu **History > Show All History**.

Lúc này, trình duyệt hiển thị thêm một cửa sổ nhỏ được tích hợp vào bên trái của trình duyệt.

3. Tại danh sách các liên kết, bạn nhấp phải chuột vào liên kết muốn xóa và chọn **Delete** (xem hình 6.28).



Hình 6.28: *Xóa History của Safari.*

Trong danh sách các liên kết được hiển thị, bạn nhấp chọn vào từng liên kết muốn xóa và chọn Delete.

VII. Xóa dấu vết trong trình duyệt Flock

Trình duyệt Flock được xây dựng dựa trên nền của Mozilla Firefox, hiện nay phiên bản mới nhất của nó là 1.0. Đây là trình duyệt có giao diện tương đối đẹp mắt và chức năng của nó cũng tương tự như Mozilla Firefox. Vì được xây dựng dựa trên nền Firefox nên cách quản lý Cookies và History cũng tương tự nên bạn có thể áp dụng cách xóa Cookies và History tương tự như đối với trình duyệt Firefox.

VIII. Xóa dấu vết trong trình duyệt Green Browser

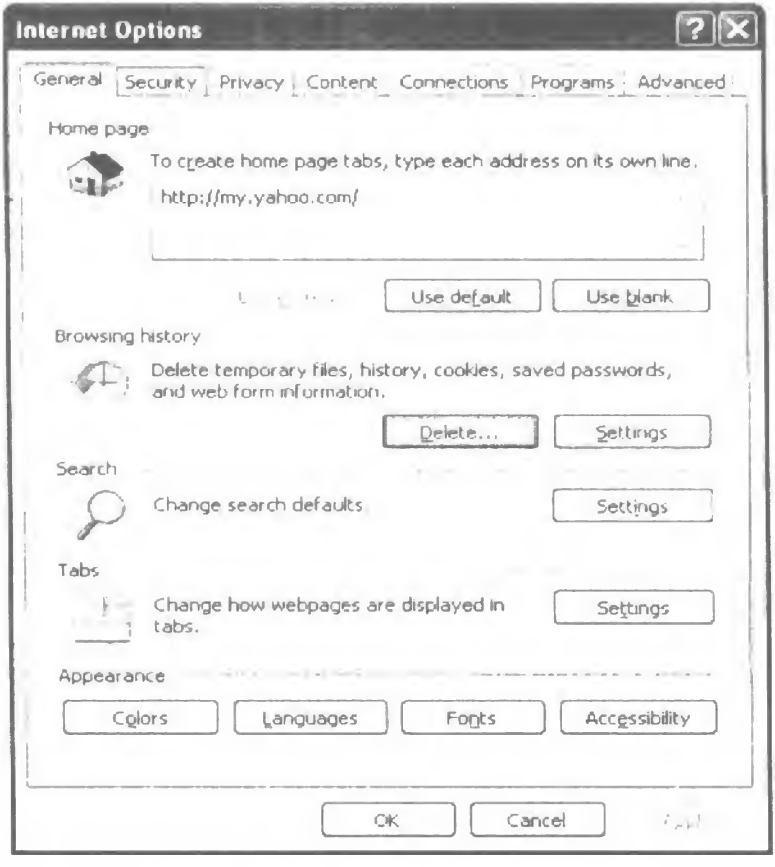
Green Browser là trình duyệt cho hệ điều hành đa nhiệm, nó được phát triển dựa trên nền của Internet Explorer (IE), nhưng có nhiều chức năng hơn IE. Hiện nay phiên bản mới nhất của trình duyệt này là 4.3.1011.

Mục này giới thiệu đến bạn cách xóa dấu vết khi truy cập Internet bằng trình duyệt này.

1. Loại bỏ Cookies

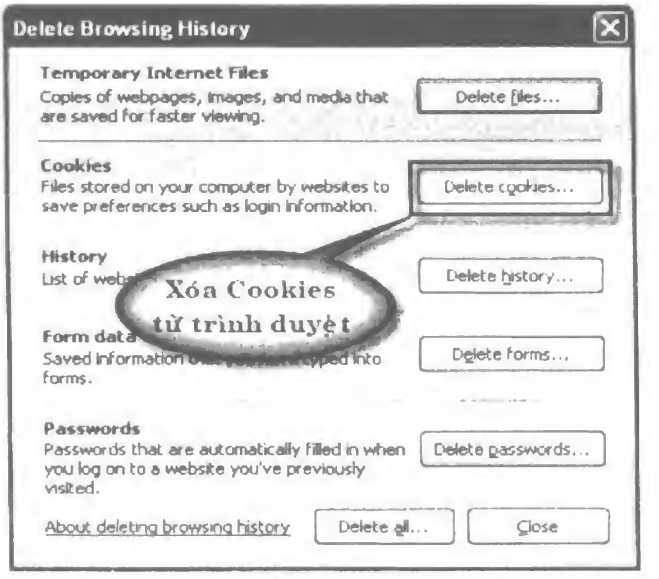
Để loại bỏ Cookies của trình duyệt Green Browser, bạn thực hiện như sau:

1. Vào **Start > Programs > GreenBrowser > GreenBrowser** để mở trình duyệt.
2. Tại giao diện chính của trình duyệt, vào menu **Tools > Internet Options** để mở hộp thoại Internet Options (xem hình 6.32).



Hình 6.32: *Hộp thoại Internet Options.*

3. Tại hộp thoại Internet Options, nhấp nút **Delete** để mở hộp thoại **Delete Browser History**, tại hộp thoại này, bạn nhấp nút **Delete Cookies** để xóa, sau đó nhấp nút **Close** để hoàn thành (xem hình 6.33).



Hình 6.33: *Xóa Cookies từ trình duyệt.*

2. Xóa History

Để xóa History từ trình duyệt Green Browser, bạn thực hiện như sau:

1. Vào **Start > Programs > GreenBrowser > GreenBrowser** để mở trình duyệt.
2. Tiếp theo, bạn thực hiện tương tự như đối với trình duyệt Internet Explorer.

IX. Xóa dấu vết trong trình duyệt Opera

Đây là trình duyệt tương đối thông dụng và mạnh mẽ trong việc duyệt Web, hiện nay Opera đã có phiên bản mới đó là 9.24. Ngoài chức năng duyệt web thông thường, Opera còn hỗ trợ download dưới dạng torrent.

Mục này giới thiệu cùng các bạn phương pháp xóa dấu vết trong trình duyệt Opera Version 9.24.

1. Xóa Cookies

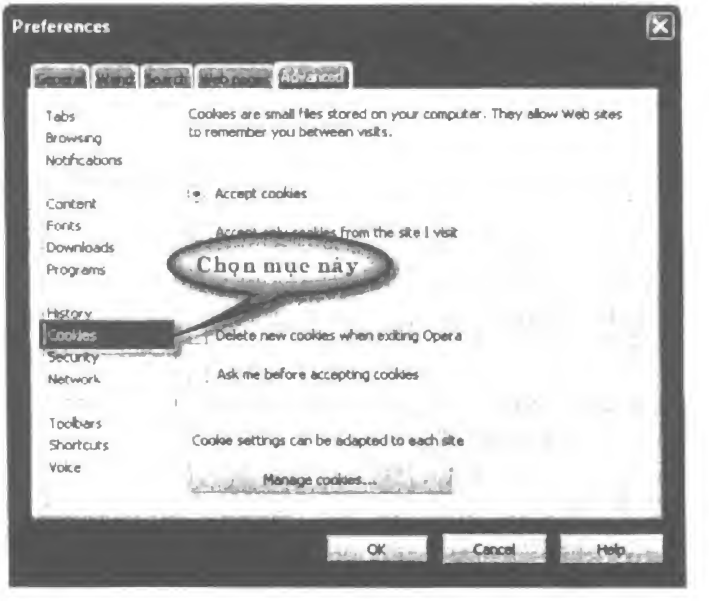
Để xóa Cookies trong trình duyệt Opera, bạn thực hiện theo các bước sau:

1. Vào **Start > Programs > Opera** để mở trình duyệt.

2. Tại giao diện chính của trình duyệt, bạn vào menu **Tools > Preferences** để mở hộp thoại **Preferences** (xem hình 6.34).

Hình 6.34: *Hộp thoại Preferences.*

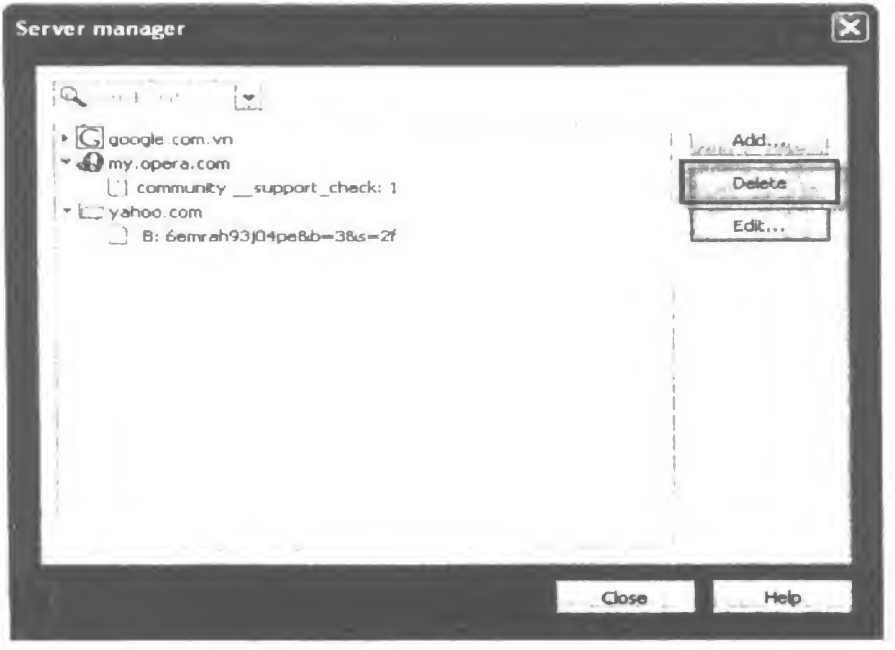
3. Tại hộp thoại Preferences, chọn thẻ **Advanced**, tiếp theo trong thẻ này tại ô bên trái, nhấp vào mục **Cookies** (xem hình 6.35).



Hình 6.35: *Thẻ Advanced trong hộp thoại Preferences.*

4. Tiếp theo, nhấp nút **Manage Cookies** để mở hộp thoại Server manager, sau đó nhấp chọn Cookies muốn xóa và nhấp nút **Delete** để xóa.

Bạn cũng có thể sửa lại Cookies bằng cách nhấp chọn Cookies, sau đó nhấp nút Edit để sửa. Ngoài ra bạn có thể tìm kiếm những thông tin cần xóa, bằng cách nhập vào hộp tìm, tiếp theo nhấn **Enter** để tìm (xem hình 6.36).



Hình 6.36: *Xóa Cookies trong trình duyệt Opera.*

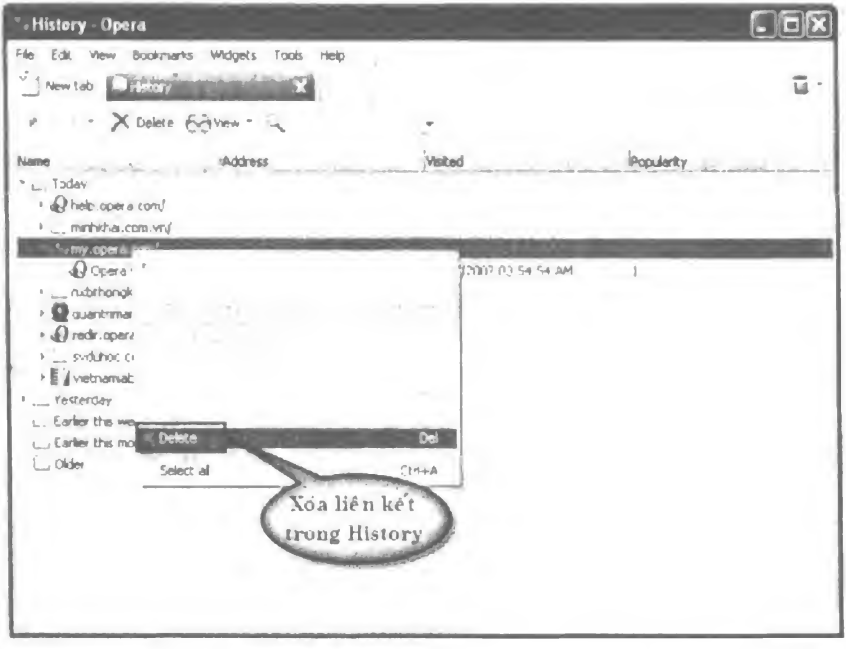
2. Xóa History

Để xóa History của trình duyệt Opera, bạn thực hiện theo các bước sau:

1. Vào **Start > Programs > Opera** để mở trình duyệt.
2. Tại giao diện chính của trình duyệt, bạn vào menu **Tools > History** hoặc nhấn tổ hợp phím **Ctrl + Alt + H** để mở cửa sổ History.

Sau khi nhấn tổ hợp phím Ctrl + Alt + H, nó sẽ hiển thị History trên một thẻ mới.

3. Tiếp theo, bạn nhấp phải chuột vào liên kết muốn xóa và chọn **Delete** để xóa (xem hình 6.37).



Hình 6.37: *Xóa History trong trình duyệt Opera.*

Như vậy đến đây ta đã hoàn thành việc xóa những dấu vết cơ bản trong máy tính và một số trình duyệt thông dụng. Ngoài ra bạn còn phải xem và sửa một số nội dung trong các tập tin .log được hệ điều hành tự động ghi lại trong Windows.

Hơn nữa đối với các ứng dụng khác nhau, sẽ có những phương pháp xóa dấu vết khác nhau. Tùy chương trình cụ thể mà bạn tìm hiểu xem những thông tin chương trình tự động ghi lại nằm ở vị trí nào trong máy tính, từ đó có những phương pháp khắc phục và xóa nhanh dấu vết thích hợp.

TỪNG BƯỚC KHÁM PHÁ AN NINH MẠNG

Tìm lại Password & phương pháp phục hồi - an toàn dữ liệu

NHÀ XUẤT BẢN LAO ĐỘNG – XÃ HỘI

Ngõ Hòa Bình 4 - Minh Khai - Hai Bà Trưng - Hà Nội

Tel: (04) 6.246.913 – Fax: (04) 6.246.915

Chịu trách nhiệm xuất bản: HÀ TẤT THẮNG

Biên tập: BAN BIÊN TẬP GIÁO TRÌNH DẠY NGHỀ

Biên soạn: VŨ ĐÌNH CƯỜNG

Sửa bản in: NGỌC AN

Trình bày bìa: VIỆT DŨNG

Thực hiện liên doanh: Công ty TNHH Minh Khai S.G

E-mail: mk.book@minhkhai.com.vn – Website: www.minhkhai.com.vn

Tổng phát hành

- Nhà sách Minh Khai: 249 Nguyễn Thị Minh Khai - Quận 1 - TP.HCM
  ĐT: (08) 9.250.590 - 9.250.591 – Fax: (08) 9.257.837
- Nhà sách Minh Châu: Nhà 30 - Ngõ 22 - Tạ Quang Bửu - Bách Khoa - Hà Nội
  ĐT: (04) 8.692.785 – Fax: (04) 8.683.995

Đại lý các khu vực

- Nhà sách Huy Hoàng: 95 Núi Trúc - Kim Mã - Ba Đình - Hà Nội
  ĐT: (04) 7.365.859
- Cty cổ phần sách thiết bị trường học Đà Nẵng: 78 Bạch Đằng - Đà Nẵng
  ĐT: 0511.837100
- Nhà sách Chánh Trí: 116A Nguyễn Chí Thanh - Đà Nẵng
  ĐT: 0511.820129
- Cty phát hành sách Khánh Hòa:
  - Nhà sách Ponagar: 73 Thống Nhất - Nha Trang - Khánh Hòa
    ĐT: 058.822636
  - Siêu thị sách Tân Tiến - 11 Lê Thành Phương - Nha Trang - Khánh Hòa
    ĐT: 058.827303
- Nhà sách Năm Hiền: 79/6 Xô Viết Nghệ Tĩnh - TP.Cần Thơ
  ĐT: 071. 821668

In 1.000 cuốn (kèm CD bài tập), khổ 16 x 24 cm,
tại Xí nghiệp in Machinco - Số 21 Bùi Thị Xuân, Q.1, TP.HCM.

Số đăng ký kế hoạch xuất bản: 47-2008/CXB/93-236/LĐXH

Mã số $\frac{93\text{-}236}{28\text{-}12}$. Quyết định xuất bản số 09/QĐ-NXBLĐXH ngày 17/1/2008

In xong và nộp lưu chiểu Quý II năm 2008.

TÌM LẠI PASSWORD

& phương pháp phục hồi an toàn dữ liệu

Giới thiệu một số sách đã xuất bản:

- macromedia FLASH 8 [tập 1, 2]
- macromedia DREAMWEAVER 8 PHẦN CƠ BẢN [tập 1, 2]
- Lập trình ActionScript cho FLASH [tập 1, 2]
- Thiết kế TRÒ CHƠI với FLASH
- AUTODESK 3DS MAX 8
- macromedia DREAMWEAVER 8 CHUYÊN NÂNG CAO
- Thiết kế web với JavaScript & DOM
- Thiết kế web với CSS
- Thiết kế khung xương cho hoạt cảnh nhân vật
- Tuyển tập THỦ THUẬT JAVASCRIPT [tập 1, 2]
- TỰ HỌC THIẾT KẾ Web [tập 1, 2]
- Thiết kế Game trong 3DS MAX
- HỌC THIẾT KẾ WEB bằng hình minh họa [tập 1, 2]
- BLOG cho mọi người [tập 1, 2]
- GIÁO TRÌNH CHỨNG CHỈ B TIN HỌC Microsoft Access 2003 [tập 1, 2]
- Thiết kế 3D trong FLASH [tập 1, 2]
- Tự học 3DS MAX
- Nhập môn Windows Vista [tập 1, 2]
- Hướng dẫn sử dụng INTERNET [tập 1, 2]
- INTERNET cho mọi nhà
- Lý thuyết CƠ SỞ DỮ LIỆU [tập 1, 2]
- SQL Server 2005 Lập trình T-SQL
- HACK INTERNET OS và bảo mật [tập 1, 2]
- SQL Server 2005 Lập trình Thủ tục và hàm
- Google [tập 1, 2]
- Phân tích thiết kế hệ thống thông tin Phương pháp & ứng dụng
- Kỹ thuật xây dựng ứng dụng ASP.net [tập 1]
- Viết SÁCH ĐIỆN TỬ? Thật đơn giản
- Thiết kế vi mạch CMOS VLSI [tập 1, 2, 3]
- TÌM LẠI PASSWORD & phương pháp phục hồi - an toàn dữ liệu

VIETDUONG

MinhKhai www.minhkhai.com.vn

UEF

NHÀ SÁCH MINH KHAI MK.PUB

Giá: 49.000 đ

8 935087 501091